MASTER EN SCIENCES INFORMATIQUES

Etude de la sécurité des architectures e-business pour les PME en fonction de leur mode d'exploitation

De Mey, Olivier

Award date:
2004

Facultés Universitaires Notre-Dame de la Paix, Namur
Institut d'Informatique
Année académique 2003-2004

Etude de la sécurité des architectures e-business pour les PME en fonction de leur mode d'exploitation

Olivier De Mey

Mémoire présenté en vue de l'obtention du grade de Maître en Informatique

Résumé :

Lors de ces dernières décennies, le secteur de l'informatique a été marqué par l'avènement et le développement des Nouvelles Technologies de l'Information et de la Communication (NTIC), qui offrent de nouvelles potentialités aux marchés existants. L'objet de ce travail s'inscrit dans le projet Acces-PME dont l'objectif est de faciliter l'accès des PME à l'e-business. Aux termes des recherches que nous avons faites, nous proposons dans ce mémoire une typologie innovantes des modes d'exploitation prenant en compte deux variables liées à la localisation : la localisation de la solution informatique d'une part, et la localisation des compétences d'autre part. A partir des travaux de V. Rosener qui définit deux types d'architectures e-business en en identifiant les composants indispensables, nous aborderons les aspects de sécurité relatifs à chacun de ces composants d'abord spécifiquement puis en les mettant en rapport avec chaque mode d'exploitation possible. Après développement, nous concluons qu'en ce qui concerne la sécurité, le mode d'exploitation le plus adéquat aux architectures e-business que nous avons défini pour la PME est le « Tout Externe ».

Mots-clés : e-business, sécurité, PME, mode l'exploitation

Abstract :

During this last decade, computer science world has been altered by Information and Communication Technology, which open new markets prospective. This research is part of the Acces-PME project, whose aim is to help SMA to deal with e-business. The researches we have made conducted us to a pioneering classification of Exploitation Mode, based on two variables related to the location: the solution itself and the knowledge needed to manage it. Based on V. Rosener's works, who defined two e-business architectures, and identified the minimum components needed in all e-business, we will go through the security issues related to each component specifically, and then related to their exploitation mode. After those researches, we will finish this thesis by showing that the most secure exploitation mode for SME e-business is All Extern.

Keywords : e-business, security, SMA, exploitation mode

Je tiens tout particulièrement à remercier mon promoteur, le Professeur Jean Ramaekers
pour son suivi attentif de mon mémoire,
ainsi que les autres professeurs et assistants qui m'ont aidé pendant mes recherches.
Je remercie Christophe Feltus, mon maître de stage,
Laurent Veuillermoz, mon chef de projet,
ainsi que l'ensemble des employés du CRPHT
qui m'ont accueilli au sein de leur entreprise
et apporté leur expérience dans leur domaine.
Enfin, je tiens à remercier mes proches pour leur précieux soutien.

Table des matières

Table des figures

Introduction

Lors de ces dernières décennies, le secteur de l'informatique a été marqué par l'avènement et le développement des Nouvelles Technologies de l'Information et de la Communication (NTIC), qui offrent de nouvelles potentialités aux marchés existants. Les entreprises qui décident de ne pas se tourner vers ces nouvelles technologies, dont l'e-business, encourent le risque de faire un manque à gagner sur les nouvelles possibilités du marché.

Il est évident que chaque entreprise, en fonction de son secteur d'activité, de sa taille ou de son chiffre d'affaire par exemple a des besoins particuliers. Dans ce travail, nous allons aborder spécifiquement le cas des entreprises qui ne disposent pas en interne de ressources suffisantes pour développer et gérer de façon efficace l'e-business. Même si ces entreprises sont en général de tailles relativement modestes, elles ne le sont pas toujours. Dans un souci de simplification, nous qualifierons ces entreprises de PME. Au sein de ces entreprises, de nombreuses questions peuvent être posées : qu'est-ce que l'e-business ? Qu'est ce qu'une architecture e-business ? Quels sont les aspects de sécurité de l'e-business ? Dois-je moi-même administrer la solution, et pourquoi ? Quels sont les coûts, les aspects juridiques ou organisationnels ? Que faut-il trouver dans un contrat e-business ? Beaucoup de questions qui, étant donné la nouveauté de ces technologies, restent bien souvent sans réponse.

Afin de répondre à ces questions, le Centre de Recherche Public Henry Tudor (CRPHT), situé au Luxembourg travaille sur un projet de recherche (le projet « Acces-PME ») qui vise à constituer un ensemble cohérent d'outils méthodologiques d'aide à l'évaluation, la spécification, le choix, le déploiement et l'exploitation de solutions sécurisées appropriées dans une optique de gestion des risques, et ce à destination des PME. Ce projet est bien entendu multi-axial. Notre mémoire s'inscrit dans le cadre de ce projet, auquel nous avons participé activement en tant que stagiaire. Concrètement, nous nous centrerons sur **les questions de sécurité liées à l'e-business des PME, et ce en fonction de l'emplacement de la solution et des compétences de gestion.**

Ce travail se structure en trois parties.
Dans la première partie, qualifiée de « partie théorique », nous décrirons « l'état de l'art », nous expliciterons de manière détaillée le cadre dans lequel s'inscrit notre recherche

(projet Acces-PME) et notre rôle concret au sein de celui-ci. Ensuite, nous définirons brièvement les concepts-clés (PME, e-business, architectures e-business, mode d'exploitation et sécurité) qui nous guiderons tout au long de ce travail. Nous consacrerons le deuxième chapitre de cette partie théorique à des considérations générales sur la notion de sécurité. Comment se définit-elle ? A quelles contraintes se trouve-t-elle confrontée ? De quels outils dispose-t-on pour l'évaluer ?

Dans notre deuxième partie, consacrée à la méthodologie, nous présenterons les modalités de nos recherches. En partant des missions qui nous furent confiées au sein du projet, nous présenterons brièvement les étapes par lesquelles nous sommes passé pour aboutir à nos observations et à nos propositions. Ces dernières feront l'objet de notre troisième et dernière partie.

Après avoir repris de manière approfondie ce que nous entendons par mode d'exploitation (sur base des recherches de Vincent Rosener s'inscrivant dans le projet Acces-PME), nous en proposerons une typologie innovante qui permet de les classer en fonction de deux critères : la localisation de la solution informatique, et la localisation des compétences. Une fois cette typologie présentée, nous définirons les différents composants d'une architecture e-business. Nous envisagerons ensuite pour chacun de ces composants les critères de sécurité en fonction de leur mode d'exploitation. Après avoir envisagé la sécurité pour chacun de ces composants, nous tenterons dans notre dernier chapitre de synthétiser ces propositions pour aboutir à des considérations générales relatives à la sécurité des architectures e-business en fonction de leur mode d'exploitation.

Partie Théorique

Chapitre 1 : « Etat de l'art », cadre de recherche et définitions

1.1. « Etat de l'art » et développements récents

Les résultats d'études internationales et l'expérience vécue sur le terrain luxembourgeois convergent vers le constat d'un accroissement considérable de l'intérêt des PME envers l'e-business. Au-delà de ce constat, ces mêmes expériences mettent en évidence que le démarrage effectif, réussi et sous contrôle, fait largement défaut sur le terrain. La raison de ce blocage est connue. En effet, il s'avère que la condition de départ pour une entreprise qui souhaite se lancer dans l'e-business est de disposer d'une architecture de communication fiable et sûre. Or, actuellement, bon nombre d'entreprises (essentiellement des PME) disposent de peu de moyens en ressources humaines, financières et techniques, et éprouvent par conséquent des difficultés insurmontables pour assurer ce premier pallier pourtant indispensable si l'on veut développer des applications e-business proprement dites. [HW99]

Les diverses approches proposées sur le plan scientifique ou sur le marché semblent peu appropriées à la réalité des PME.

Les solutions intégrées 'clé sur porte' pour le cas d'une PME isolée présentent l'inconvénient d'un prix élevé, d'un manque de standardisation et d'une complexité difficile à maîtriser en interne, et ce non seulement en matière de choix et de déploiement mais aussi et surtout en matière d'exploitation.

Les solutions d'externalisation complète de la fonction e-business (plate-forme et applications) ne portent quant à elles que sur des modèles limités et génériques d'e-business. Elles posent la question des facteurs de différenciation concurrentielle de l'entreprise, ne règlent pas toutes les questions de spécificités techniques, fonctionnelles et organisationnelles, ni tous les problèmes de sécurisation et de responsabilité dans la relation de l'entreprise avec son fournisseur e-business. [HW99]

D'un autre côté, l'initiative du logiciel libre (open source) gagne sans cesse du terrain et on trouve de plus en plus de composants de sécurité prêts à être réutilisés. Pour une PME,

l'intérêt de solutions basées sur ces composants est bien sûr le faible coût, mais aussi le bénéfice de rester dans des solutions ouvertes. Cependant, le manque d'informations et de compétences techniques ne permet pas le développement satisfaisant de telles solutions pour PME.

Face à ces diverses approches et aux limites qu'elles présentent, on peut conclure que le prêt à l'emploi ou « plug and play » e-business reste une illusion. La nécessité d'une démarche rigoureuse dans la spécification, le choix, le déploiement et l'exploitation des solutions est indéniable. [HW99]

Or, il convient de mettre l'accent sur le déficit dans l'offre de services de sécurisation informatique au Grand-Duché de Luxembourg et plus largement en Europe. Si le marché des composants libres en matière de sécurisation est en pleine expansion, si des standards internationaux d'architectures sécurisées se dégagent, si des modèles d'exploitation diversifiés sont proposés, si des méthodes et techniques de risk management permettent de plus en plus d'évaluer les situations, de spécifier les solutions et de les déployer de manière rigoureuse, il est presque impossible à un prestataire isolé, même de taille importante, de mobiliser les différentes disciplines techniques, organisationnelles et juridiques permettant d'intégrer ces différents résultats. [HW99]

Pour ce qui concerne les démarches méthodologiques, une enquête réalisée par le CLUSSIL (http://www.clussil.lu) montre clairement que les approches des experts relatives à la sécurité informatique portent encore sur des questions exclusivement techniques et parcellaires et que les considérations globales et méthodologiques font largement défaut.

Lorsqu'il s'agit de prestataires informatiques qui s'adressent à la PME, le constat est encore plus clair. Les résultats cités plus haut, même s'ils pouvaient être maîtrisés par ces prestataires resteraient largement surdimensionnés au cas spécifique de la PME et nécessiteraient des approches de déploiement et d'exploitation nouvelles.

Pour finir de brosser ce tableau de la situation, il faut également avouer que, lorsqu'une telle offre de qualité à destination des PME existera, ce à quoi le projet Acces-PME va tenter d'aboutir, la reconnaissance de sa valeur ajoutée par les chefs d'entreprise sera encore loin d'être acquise et nécessitera un effort considérable de sensibilisation. S'il est entré dans la pratique du dirigeant de PME de faire appel à des services intellectuels par exemple de type

fiscaliste, peu nombreux sont ceux qui sont prêts à investir dans une mission dont l'objectif serait la garantie de la qualité et la sécurité de son infrastructure informatique. [HW99]

1.2. Cadre de recherche : Projet Acces-PME

Le projet ACCES-PME porte sur l'infrastructure sécurisée dans le contexte particulier des PME souhaitant intégrer différentes formes d'e-business (B2C, B2B). Ce projet de recherche étudie les solutions sécurisées en vue de les rendre accessibles à des PME dans une forme exploitable sans risque.

Les solutions étudiées se situent à deux niveaux : premièrement au niveau du choix de plates-formes et composants logiciels sécurisés, et plus particulièrement ceux issus de la communauté du logiciel libre, et deuxièmement au niveau des diverses formes d'exploitation sécurisée de ces solutions e-business allant d'un hébergement interne à l'externalisation complète du service.

Ce projet aborde les aspects techniques, organisationnels et juridiques de manière interdisciplinaire. Fondé sur un travail rigoureux d'identification des exigences et des spécificités des PME en matière d'e-business sécurisé, ce projet vise à constituer un ensemble cohérent d'outils méthodologiques d'aide à l'évaluation, la spécification, le choix, le déploiement et l'exploitation de solutions sécurisées appropriées dans une optique de gestion des risques. [HW99]

De cette façon, l'ensemble des compétences et connaissances nécessaires au choix et à l'exploitation de solutions sécurisées pour PME est intégré dans des « packages méthodologiques » conçus en tenant compte des exigences spécifiques des PME et, notamment, des capacités pour leurs conseillers à les utiliser. A ce titre, le projet a pour finalité de concevoir les délivrables qui seront disséminés dans le cadre d'un projet conventionné qui dynamisera le marché du conseil et du service informatique pour l'exploitation sécurisée de plates-formes e-business pour PME. [HW99]

L'objectif central du projet concerne une méthode de risk management pour l'évaluation, la spécification et le déploiement d'une plate-forme d'e-business. Pour assurer la qualité, la pertinence et l'atteinte de cet objectif, le projet devra produire des outils méthodologiques pour l'exploitation des résultats du projet avec une approche de type risk management. Ces

outils assisteront les consultants chargés de l'analyse des risques et du choix de l'architecture sécurisée adéquate aux exigences de l'entreprise.

Après avoir posé le cadre global dans lequel s'inscrit notre mémoire, nous allons à présent définir les concepts qui nous guideront dans la suite de ce travail.

1.3. Définitions

Avant de passer concrètement aux définitions, une remarque s'impose. Dans notre domaine, il est souvent difficile -voire impossible- d'avoir une définition univoque d'un concept. En effet, selon l'auteur ou la source, les acceptations que l'on peut avoir d'un concept varient fortement. Dans le cadre de ce travail, les définitions que nous avons choisi de retenir s'inscrivent dans le projet Acces-PME. Cette remarque étant faite, voyons ce que nous entendons par PME, par e-business, par architectures e-business, par mode d'exploitation et enfin, par sécurité.

1.3.1. PME

Traditionnellement, le terme de Petites et Moyennes Entreprises se définit soit par rapport au nombre de personnes la constituant, soit par rapport au chiffre d'affaire de l'entreprise, ou encore, dans le secteur informatique, par le nombre d'écrans en son sein. Dans le cadre qui nous occupe, il va de soi qu'une très petite entreprise constituée de cinq ingénieurs informaticiens peut être capable de gérer elle-même son informatique, alors qu'une grosse administration de 200 personnes ou un hôpital peut n'avoir aucune connaissance informatique. Ce qui nous intéresse ici, c'est moins la question de la taille de l'entreprise que la question de savoir si elle a les compétences nécessaires pour gérer une solution informatique. Bien que ces deux variables soient souvent liées, elles ne le sont pas toujours. Par conséquent, nous qualifierons de PME « *toute entreprise n'ayant pas d'informaticien ou de service informatique interne dédié*»

1.3.2. E-business

La définition de l'e-business que nous utiliserons est basée sur un travail de V. Rosener [Ro04], dont la tâche, au sein du projet Acces-PME, a été de donner une définition de l'e-business, de recenser les architectures e-business, de proposer une méthode de qualification d'architecture et d'évaluer des architectures e-business sur le plan de l'assemblage des composants (compatibilité des interfaces et contraintes techniques) tout en assurant la validité vis-à-vis des exigences de sécurité. La définition de l'e-business et les architectures que nous présenterons nous ont été données telles quelles, et constituent une des bases principales de ce document.

Comme le montre la figure [Fig. 1.1], l'e-business est un sous-ensemble d'un « Business » plus général. Ce business définit un marché, il a des revenus et des propositions de valeurs pouvant être des produits ou des services [Fig. 1.2]. Ce business réalise un ensemble d'activités. Il respecte des lois, utilise des ressources, et implique des participants qui peuvent être [Fig. 1.3] une administration, une entreprise ou une personne physique. Chacun de ces participants joue au moins un rôle : client ou fournisseur.

L'e-business quant à lui est constitué de l'e-commerce, l'e-broker, l'e-facilities et de l'e-advertising. Dans cette définition, l'e-communication et l'e-administration sont considérées comme des « e-activities », et non pas comme de l'e-business.

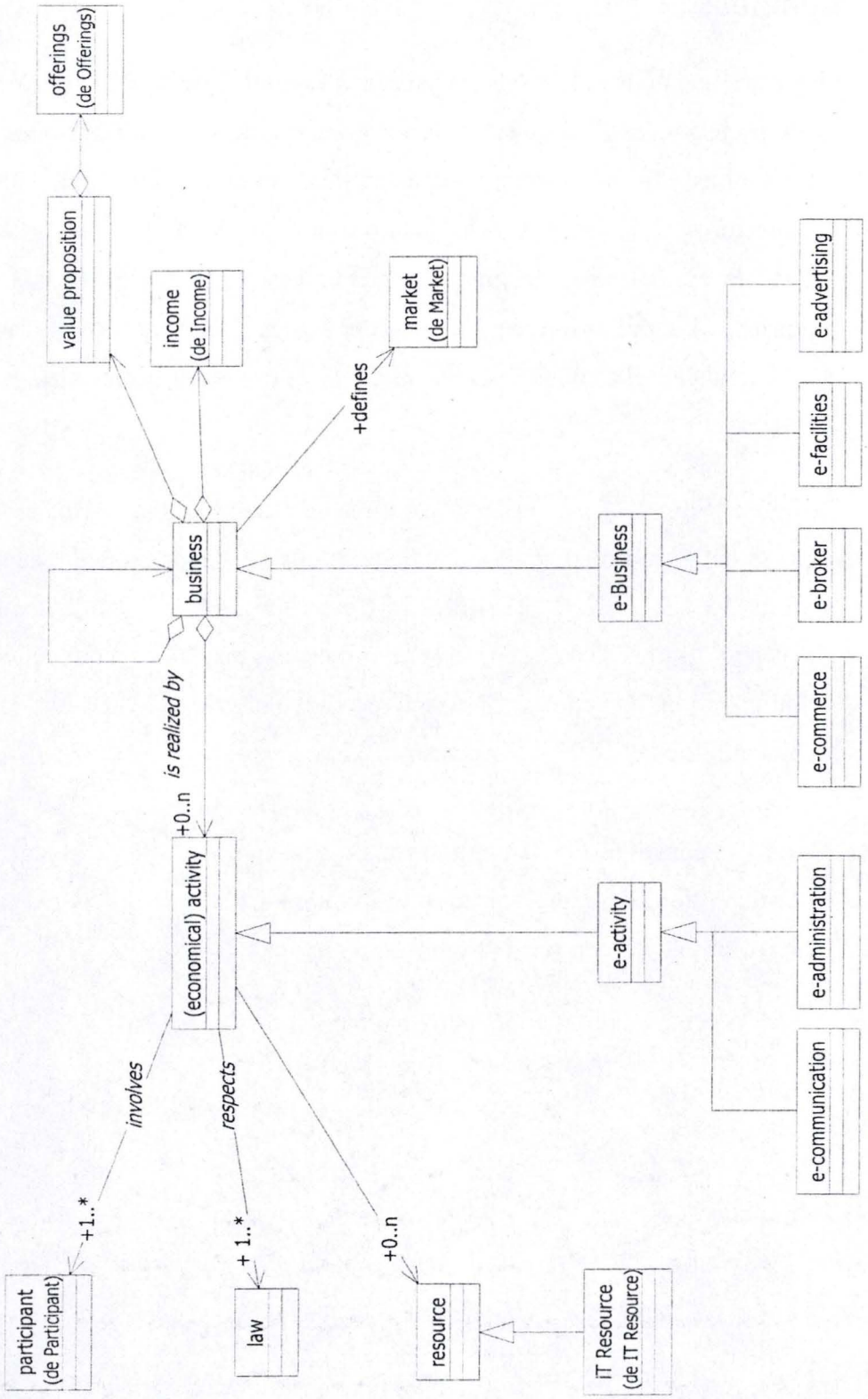

Fig. 1.1 – e-business

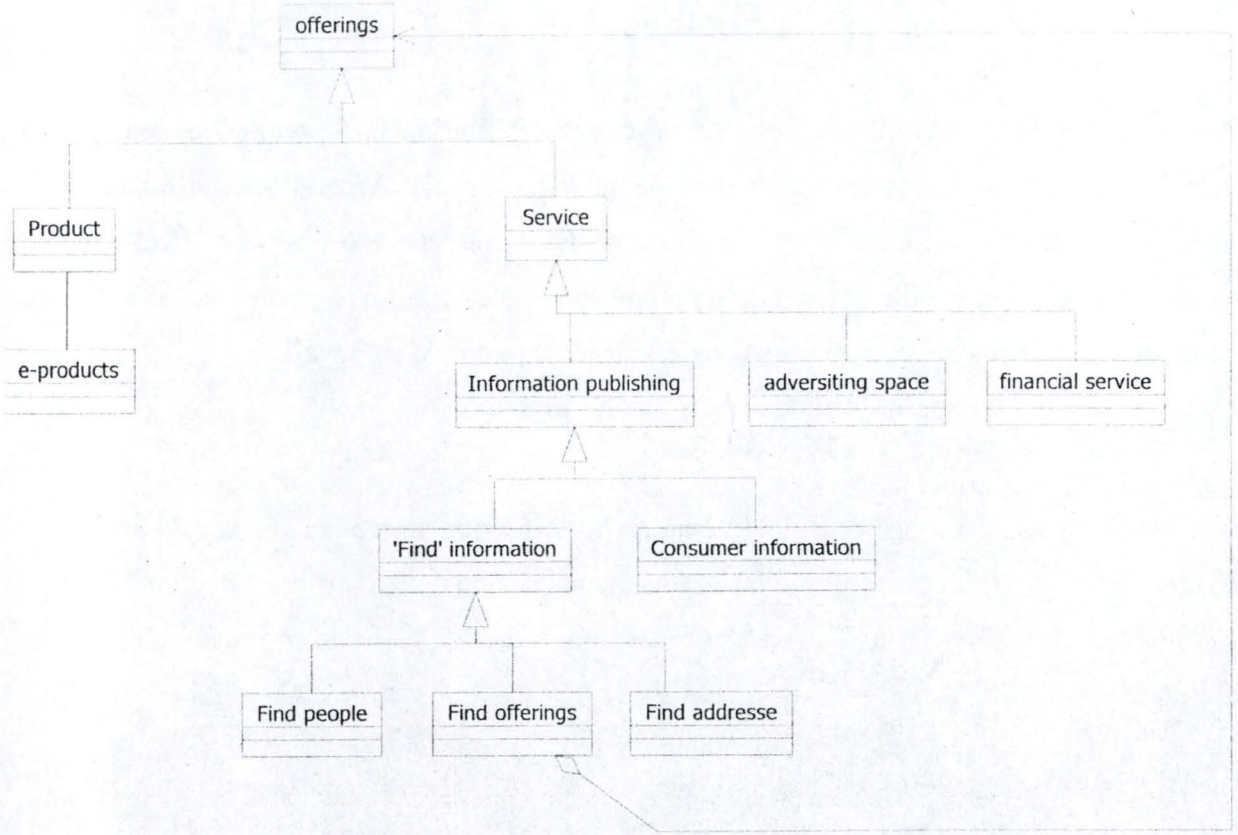

Fig. 1.2 – offerings

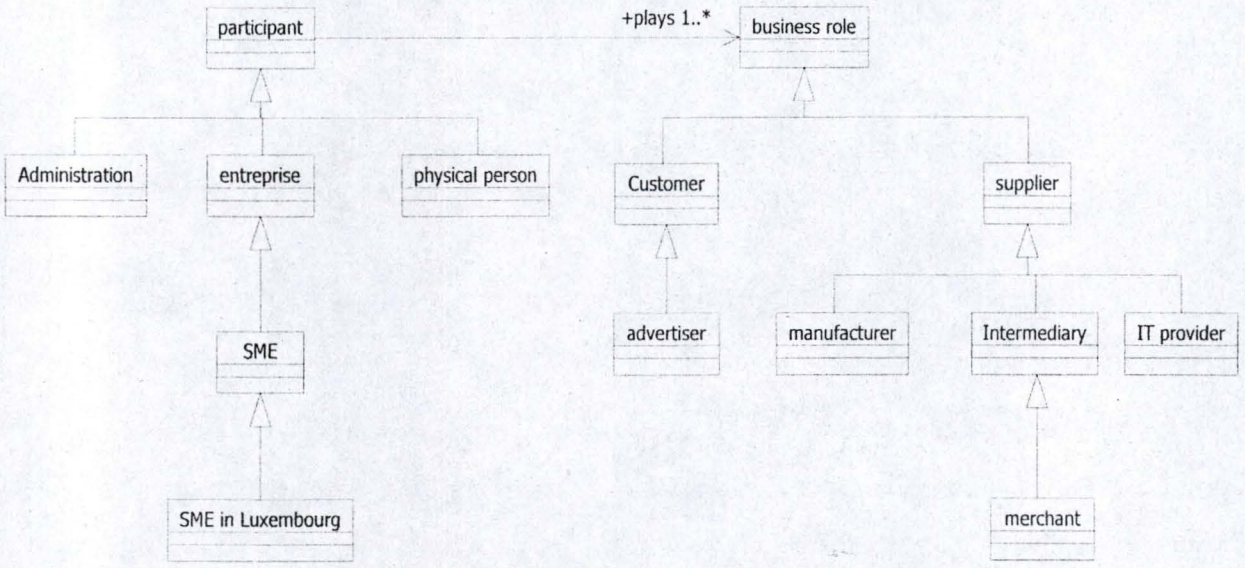

Fig. 1.3 - participants

1.3.3. Architectures e-business

Dans le cadre de ce travail, nous choisirons comme définition de l'architecture e-business celle développée par V. Rosener dont la tâche au sein du projet Acces-PME fut notamment, rappelons-le, de définir l'e-business et de recenser les architectures e-business. Il définit les architectures par l'ensemble des composants indispensables à la mise en œuvre d'e-business. Nous reviendrons sur ces composants dans la troisième partie de ce travail.

1.3.4. Mode d'exploitation

A nouveau, il n'existe pas dans la littérature de définition univoque ou de classification exhaustive des « modes d'exploitation ». Nous avons décidé de retenir l'acceptation suivante : le mode d'exploitation est la mise en œuvre technique et le suivi d'une solution informatique afin d'en assurer la pérennité. Ce que nous appelons la solution informatique sont le logiciel, le matériel nécessaire à son utilisation, et leur documentation.

Bien que ce concept puisse renvoyer à de multiples aspects, le terme « Mode d'Exploitation » renvoie dans notre propos à la localisation de la solution et des compétences nécessaires pour gérer cette solution. Il nous semble en effet que la localisation d'une solution et des compétences pour la gérer constituent un élément fondamental de la sécurité de cette solution.

Nous reviendrons plus loin sur une définition plus détaillée de la notion de Mode d'exploitation ainsi que sur une proposition de typologie.

1.3.5. Sécurité

Parler de sécurité revient à envisager trois aspects : la confidentialité, l'intégrité et la disponibilité. Etant donné que la sécurité est au cœur de ce travail, nous avons décidé de développer cette notion plus en profondeur et d'en faire l'objet du chapitre suivant.

Chapitre 2 : Sécurité : exigences, contraintes et méthodes d'évaluation.

La sécurité informatique d'une plate-forme e-business est un problème global. Une règle communément admise dit que la sécurité d'un système informatique est aussi élevée que le niveau de son composant le plus faible [Gh99]. Nous avons donc un problème étendu à tout un système : les gens pensent souvent que le plus important à sécuriser est le transport de l'information, alors que le client, le serveur, et le système d'exploitation nécessitent une attention tout aussi importante.

2.1 Les exigences classiques

Comme nous l'avons évoqué ci-dessus, les exigences de la sécurité des systèmes d'informations considérées classiquement sont de garantir la confidentialité, l'intégrité et la disponibilité de l'information.

a) Confidentialité

La confidentialité constitue la garantie que l'accès aux informations sensibles ou confidentielles n'est autorisé qu'aux entités, individus et processus autorisés.

b) Intégrité

L'intégrité constitue la garantie que l'information est exhaustive, exacte et résulte d'activités autorisées. Dans le cadre de communications électroniques, elle consiste donc à s'assurer que le message transmis n'a pas été modifié durant sa transmission. L'intégrité a deux facettes : l'intégrité des données, ou la garantie que les données n'ont pas été altérées de façon non autorisée pendant leur stockage, leur transport et leur traitement; et l'intégrité des systèmes, ou la garantie qu'un système exécute ses activités de façon normale, librement d'une exploitation non autorisée.

c) Disponibilité

La disponibilité caractérise la capacité de mise à disposition de l'information dans des conditions définies de temps et de performance.

Aux exigences traditionnelles se rajoutent aujourd'hui deux autres exigences : l'imputabilité et l'authenticité. L'imputabilité est la possibilité de tracer les actions réalisées sur un système par un individu ou une entité informatique afin de déterminer d'éventuelles responsabilités en cas d'incident. L'authenticité, quant à elle, est la possibilité de garantir l'origine de l'information. [Ke03]

2.2 Les contraintes de la sécurité

La sécurité ne se limite pas aux définitions données. En effet, si elle a des objectifs précis, elle doit également obéir à certaines contraintes. Elle doit être un support aux missions de l'organisation. En effet, le système d'information de l'organisation est de plus en plus souvent une ressource critique dans le support de ses missions. Sa protection est donc vitale pour la pérennité de l'organisation.

a) La sécurité doit être un élément du management de l'organisation :

Le niveau de sécurité requis pour assurer les missions de l'entreprise doit être déterminé par le management.

b) La sécurité doit être rentable :

Les solutions de sécurité ne devraient être choisies que si elles ont un coût inférieur à la simple acceptation du problème. En investissant de façon rationnelle dans des mesures de sécurité, une organisation peut réduire la fréquence et la sévérité des pertes liées à l'insécurité informatique.

c) La sécurité requiert une approche intégrée :

Pour fonctionner de manière efficace, les contrôles de sécurité dépendent souvent du fonctionnement d'autres contrôles avec lesquels existent des dépendances. Pour autant qu'ils soient choisis de façon appropriée, les contrôles opérationnels, techniques et de gestion devraient fonctionner en synergie. En général, ces interdépendances sont difficiles à

appréhender. Pourtant, leur compréhension est essentielle à la mise en œuvre d'une sécurité efficace.

L'efficacité des contrôles de sécurité dépend aussi d'autres facteurs comme le management, les aspects légaux, les certifications qualité et les contrôles internes. La sécurité informatique doit donc fonctionner en accord avec les dispositions propres à l'entreprise.

d) La sécurité doit respecter les droits des individus :

Dans cette perspective, les mesures de sécurité doivent être choisies et implémentées en accord avec le respect des droits et des intérêts légitimes des tiers, ce qui implique la mise en balance des besoins de sécurité avec les besoins des propriétaires et utilisateurs de l'information ainsi que des objectifs stratégiques et politiques de l'organisation. En outre, certains contrôles de sécurité sont contradictoires avec le respect de la vie privée. De plus, certaines nécessités politiques au niveau des états peuvent limiter l'applicabilité de certains contrôles. Les contrôles de sécurité doivent donc être choisis et implémentés en gardant à l'esprit les droits et intérêts légitimes des tiers qui interagissent avec le système. [Ke03]

e) La sécurité doit faire l'objet de formation ou d'informations spécifiques :

Les droits et les devoirs du personnel en tant qu'utilisateurs du système d'information doivent être clairement définis. Tout utilisateur du système d'information doit être informé de ses obligations vis à vis du système informatique.

f) La sécurité doit être périodiquement réévaluée :

En effet, les systèmes d'information évoluent dans un environnement technologique très dynamique dont les risques -et donc les exigences de sécurité- sont en constante évolution. Il importe donc de réévaluer régulièrement les mesures prises en fonction de l'impact de l'introduction de nouvelles technologies.

Avant de passer aux méthodes d'évaluation, nous voudrions mettre en garde le lecteur par rapport à des idées reçues sur la sécurité. En effet, les problèmes couramment référencés proviennent souvent de l'extérieur de l'entreprise, mais il nous semble important de rappeler que des menaces internes existent elles aussi. Les principales menaces sont le vandalisme et le sabotage, la perte de confidentialité, les vols et les fraudes, la violation de l'intégrité des données, et les attaques de type Denial of Service (DoS). Au niveau du serveur, il ne faut pas

croire que le fait d'utiliser des protocoles d'encryption résoudra les problèmes de confidentialité ; car même s'ils fournissent un niveau raisonnable de confidentialité lors du transfert des données, ces données seront enregistrées en « clair » dans une Base de Données. Dès lors que le serveur Web sera mal configuré, un accès à cette Base de Données réduirait à rien les efforts mis en œuvres par lesdits protocoles. De plus, une fois la confidentialité garantie, il faut aussi s'assurer qu'un pirate ne puisse détruire tout simplement les informations contenues dans la Base de Données. En effet, cette Base de Données contient les informations les plus critiques de l'entreprise : listings de clients, adresses, historiques des transactions, numéros de cartes de crédit, … Une attaque compromettant la confidentialité de ces informations pourrait mettre à mal cette entreprise, en lui faisant perdre sa clientèle, et la confronterait à des problèmes juridiques potentiels. De même, une attaque DoS peut provoquer, même sur une structure ne fonctionnant pas en temps réel, une perte financière importante. [Gh99]

Après avoir défini la sécurité en termes d'exigences et de contraintes, nous allons exposer trois normes de validation existant sur le marché.

2.3 Méthodes d'évaluation

Les normes de sécurité sont apparues dans les années '80, alors que l'on se demandait comment évaluer la sécurité d'un système, ou tout simplement d'un programme. Dans les années '70, cela se faisait avec des équipes de hackers dont le but était de déceler des failles de sécurité. Nous pouvons distinguer trois normes principales pour la validation de la sécurité d'un logiciel. Nous allons les citer et en expliquer les principes généraux de fonctionnement. Notons que la maîtrise de ces normes demande un travail qui dépasse largement le cadre de notre propos, et que nous ne les exploiterons dès lors pas davantage.

2.3.1 Orange Book

En 1983, le Departement of Defense (DoD) et le National Computer Security Center se sont rassemblés pour écrire le célèbre « orange book ». C'est un ouvrage clair et concis. Il donne des directives pour les designers, et ne traite que des systèmes « classiques ». Il ne décrit pas le processus d'évaluation, et il n'y a pas de chance d'évolution d'évaluation.

Les résultats d'évaluation de programmes vont de D à A :
D : protection insuffisante
C1 et C2 : Protection facultative
B1, B2, B3 : Protection obligatoire
A1, A2 : Protection certifiée
[Li04]

En 1991, l'Europe à décidé d'établir ses propres standards, et a créé l'ITSEC.

2.3.2 ITSEC

Les "Information Technology Security Evaluation Criteria" (ITSEC) sont des standards développés en Europe. Leur but est de démontrer la conformité d'un produit ou d'un système (référencé dans la norme comme le « Target of Evaluation », ou le TOE). Le TOE est évalué pour savoir si l'implémentation est efficace et correcte. La certification ITSEC est effectuée par un tiers, appelé « commerical licensed evaluation facility » ou CLEF.

Comme le montre la figure [fig. 1.4], le processus d'évaluation ITSEC se déroule comme suit : le commanditaire (typiquement le développeur) d'un TOE choisit un CLEF. Le CLEF évalue la cible de sécurité et produit un plan de travail. Il nomme un certificateur, et le travail peut commencer. Le commanditaire fournit à l'évaluateur un ensemble complet de délivrables, et il vérifie si ceux-ci répondent aux exigences des critères en terme de complétude, de consistance et d'exactitude. Si l'évaluateur est satisfait, un rapport est produit. Il est soumis au certificateur pour son approbation. Si le certificateur est aussi satisfait, un rapport de certification est produit, et un certificat ITSEC est attribué. [Ry04]

Les responsabilités du commanditaire sont multiples : il doit trouver les fonds pour l'évaluation, payer pour le CLEF et pour le certificateur. Le commanditaire doit aussi produire un ensemble de délivrables, et doit également fournir à l'évaluateur et au certificateur tous les matériaux requis pour l'évaluation. [Ry04]

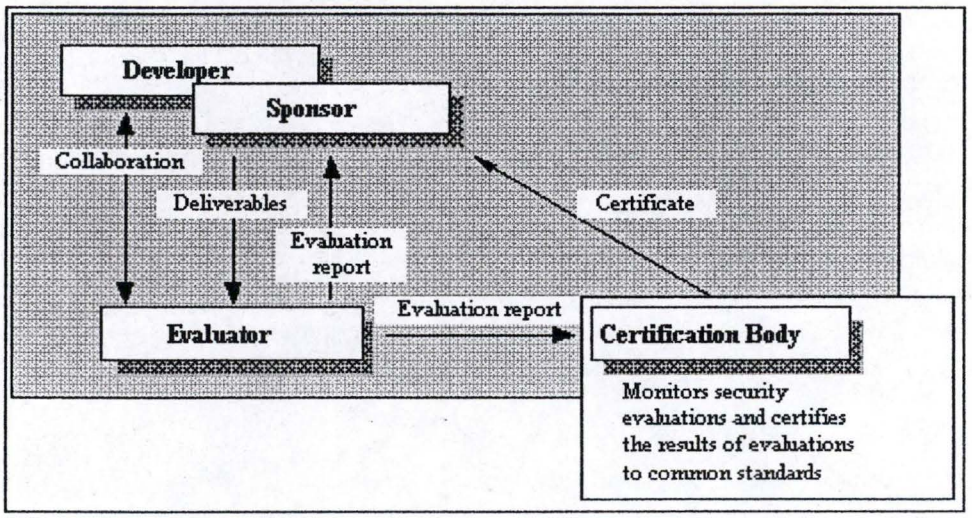

Fig. 1.4 – Certification ITSEC

L'ITSEC propose une approche cohérente et systématique pour examiner comment la sécurité a été prise en compte durant le design, le développement, l'installation et l'exploitation d'un produit ou d'un système.

Six niveaux de conformités sont définis. Les conditions pour l'évaluation sont données du niveau le plus clément (niveau E1) au niveau le plus rigoureux (niveau E6) pour un produit de très haute sécurité. Le tableau suivant illustre les rigueurs des différents niveaux ITESEC.

Granularité d'information de conception requise pour l'évaluation:

Tableau 1.1 – Granularité d'information de conception requise pour l'évaluation

Niveau	Information de conception requise
E1	conception architecturale.
E2	conception architecturale et conception détaillée.
E3 et supérieurs	conception architecturale, conception détaillée, code source ou schémas de matériel.

Différents modèles des spécifications:

Tableau 1.2 – Modèles des spécifiations

Niveau	Modèle de spécifications
E1, E2, E3	documentation informelle.
E4, E5	Modèle formel fondamental de la politique de sécurité, spécifications semi formelles de la sécurité, descriptions semi formelles de l'architecture et design détaillé.
E6	Modèle formel fondamental de la politique de sécurité, spécifications formelles de la sécurité, description formelle de l'architecture et description semi formelle du design détaillé.

Les critères d'évaluation sont employés pour l'évaluation d'une gamme très large de produits de sécurité ou de systèmes. Ils portent sur la sécurité réellement fournie par le produit et ils vérifient que ces fonctions sont développées proprement et qu'elles fournissent le service prévu. [Ce04]

Les trois étapes principales de l'approche d'évaluation sont:

- l'analyse de l'efficacité: déterminer la pertinence des fonctions de sécurité du système et ses possibilités de résister à des actions malveillantes ;
- l'analyse de l'exactitude: assurer que le système développé soit en accord avec les objectifs de sécurité ;
- les tests: les étapes précédentes permettent à l'expert d'identifier et de se concentrer sur les cas d'essais les plus significatifs concernant la résistance du système.

Les activités d'évaluation qui seront exécutées pendant la phase d'évaluation sont identifiées par la liste suivante, qui ne prétend pas à l'exhaustivité:

- Vérifier l'analyse de convenance,
- Vérifier l'analyse obligatoire,
- Examiner la force des mécanismes,
- Examiner les vulnérabilités de construction,
- Examiner la facilité d'utilisation,
- Vérifier les requirements,
- Vérifier la conception architecturale,
- Vérifier la conception détaillée,
- Vérifier l'exécution,
- Vérifier l'environnement de développement,
- Vérifier la documentation opérationnelle,
- Vérifier l'environnement opérationnel.

[Ce04]

Quelques années plus tard, le Canada, les Etats-Unis et l'Europe se sont réunis pour créer des critères internationaux: les Common Criteria.

2.3.3 Common Criteria

a) Vue d'ensemble

Les Common Criteria (CC) sont des standards internationaux dont le but est de permettre aux organisations de démontrer la conformité d'un produit à une cible de sécurité.

b) Profils de Protection

Un profil de protection (PP) est un document qui concerne un groupe particulier de produits IT (ex : firewall, réseaux privés virtuels, etc.). Les PP fournissent des menaces spécifiques et des conditions fonctionnelles qui sont applicables pour leur type spécifique de produit IT. Quand un PP est produit, il est créé selon un « Evaluation Assurance Level» spécifique. Un produit qui prétend être conforme à un PP doit remplir toutes les conditions fonctionnelles exigées par celui-ci. Un produit peut également dépasser le PP en ajoutant des menaces et des conditions additionnelles ; pour autant que toutes les conditions du PP soient satisfaites. [Co04]

c) Evaluation Assurance Level (EAL)

Il y a sept niveaux d'assurance auxquels un produit IT peut être évalué. Les sept niveaux déterminent la quantité de documentation d'assurance exigée pour l'évaluation, 1 en exigeant le moins, et 7 le plus. [Co04]

EAL1 - fonctionnellement examiné
EAL2 - structurellement examiné
EAL3 - méthodiquement examiné et vérifié
EAL4 - méthodiquement conçu, examiné, et passé en revue
EAL5 – semi formellement conçu et examiné
EAL6 - conception semi formellement vérifiée et examinée
EAL7 - conception formellement vérifiée et examinée

La documentation exigée entre dans un certain nombre de catégories : Gestion de configuration, livraison et opération, développement (spécifications, conception, et code

source), documents de conseils (manuels d'utilisateur), appui de cycle de vie (adhérence à une méthodologie bien définie de développement), essais et enfin, évaluation de vulnérabilité. [Co04]

Après avoir posé le cadre dans lequel s'inscrit ce travail et avoir proposé des définitions des concepts-clés, nous allons dans la seconde partie de ce travail envisager les aspects méthodologiques.

Deuxième Partie - Méthodologie

En tant que stagiaire au CRPHT, nous avons participé au projet Acces-PME dont l'objectif général est de favoriser l'accès des PME à l'e-business. Ce projet avait débuté bien avant notre arrivée, et se poursuit encore à l'heure actuelle. Il nous semble intéressant, afin que le lecteur comprenne bien notre apport à ce projet, d'en retracer très brièvement les étapes. En effet, les développements que nous proposons dans la partie suivante n'auraient pas été possibles s'il ne s'inscrivait dans un travail d'équipe où les contributions de chacun furent primordiales.

Le projet se déroule globalement en cinq étapes. Les deux premières sont liées à la définition de la sécurité. Nous avons repris les éléments principaux de cette définition dans notre partie théorique. D'autres professionnels -dont V. Rosener- ont ensuite été chargés de définir l'e-business et les architectures e-business. Cela constitue la troisième étape. La quatrième étape porte sur l'étude des modes d'exploitation des architectures e-business sous l'angle des contraintes de sécurité, des contraintes organisationnelles, des contraintes de coûts, et des contraintes juridiques et contractuelles. La dernière partie de ce projet, sur base des quatre étapes préalables, sera de constituer un ensemble cohérent d'outils méthodologiques d'aide à l'évaluation, la spécification, le choix, l'exploitation et la diffusion de solutions sécurisées afin que les PME puissent utiliser l'e-business de façon optimale.

Notre rôle au sein de ce projet, rôle que nous avons choisi d'exposer dans ce mémoire, se situe dans la quatrième étape. En effet, nous devions faire l'étude de **la sécurité** des architectures en fonction des « modes d'exploitation ».

Voici comment nous avons procédé. Dans un premier temps, nous avons proposé une typologie des modes d'exploitation en lien avec la localisation. Il apparaît en effet qu'il n'existe pas à ce jour d'études consacrées à l'analyse du déploiement d'une solution et du suivi de cette dernière en fonction de l'emplacement géographique de la solution et des compétences nécessaires pour la gérer. Or cette idée de localisation nous semblait importante, et porteuse d'une grande valeur ajoutée. Dans la mise au point de cette typologie, notre liberté fut grande. Nous avons commencé par rechercher sur Internet différentes solutions informatiques en tous genres (Serveur Web, ERP, Base de Données, CRM, etc.). Il va sans dire que ces recherches furent laborieuses. Face à la multitude d'informations, il nous a fallu réfléchir à des variables qui nous permettraient de classifier toutes ces solutions. Nous

présenterons dans la partie suivante le fruit de ces réflexions ainsi qu'une proposition de typologie mettant en évidence quatre modes d'exploitation.

Notons que cette typologie sera la base de travaux ultérieurs. En effet, d'autres personnes traiteront des contraintes organisationnelles, juridiques, contractuelles et financières en fonction du mode d'exploitation de l'architecture.

Après avoir défini quatre modes d'exploitation, il nous a fallu analyser la sécurité de l'architecture en fonction de son mode d'exploitation. Nous avons décidé de diviser l'étude en deux temps.

Premièrement, nous avons défini chaque composant et avons décrit certains aspects de sécurité qui y sont liés en nous basant sur les ouvrages [Gh99], [An01] et [Ga02]. Pour chaque composant, nous avons sélectionné un échantillon de solutions existantes, en prenant garde à ce qu'un maximum de modes d'exploitation soient répertoriés. Nous avons établi ensuite pour chaque composant une liste de questions (une grille d'observation) auxquels nous avons répondu pour chaque solution trouvée. Vous trouverez en annexe ces listes ainsi que le détail des réponses aux questions. Une fois ces observations récoltées, nous avons séparé les solutions sur base de leur mode d'exploitation, et avons recherché d'éventuelles similitudes et différences afin de caractériser au mieux chaque mode d'exploitation pour le composant en question.

Après avoir fait cet exercice pour chacun des composant, nous avions une idée précise des aspects de sécurité de chaque composant en lien avec les différents modes d'exploitation possibles.

Il nous a ensuite fallu faire l'évaluation de la sécurité des architectures en fonction de leur mode d'exploitation, en envisageant alors l'architecture comme un tout.

Voici dans les grandes lignes la manière dont nous avons construit notre travail. Dans la partie « recherche », nous détaillerons ces étapes, et nous présenterons nos résultats.

Troisième Partie - Recherches

Chapitre 1 : Modes d'Exploitation

Comme annoncé, après avoir rappelé l'acceptation que nous avons du terme « mode d'exploitation », nous allons présenter notre typologie et distinguer quatre modes d'exploitation. Nous affinerons ensuite davantage cette définition, et présenterons une représentation schématique de cette classification. Pour finir cette partie, nous expliquerons la notion de « housing », qui doit être étudiée indépendamment d'une solution particulière.

1.1. Première classification

Comme nous l'avons défini, un Mode d'Exploitation est la mise en œuvre technique et le suivi d'une solution informatique afin d'en assurer la pérennité. Rappelons que par « solution informatique », nous entendons le logiciel et le matériel nécessaire à son utilisation.

Partant du postulat que la localisation est une variable importante, nous allons distinguer les modes d'exploitation les uns des autres par deux variables : la localisation de la solution informatique et la localisation des compétences nécessaires pour la gérer. En combinant ces deux variables, nous pouvons définir quatre modes d'exploitation que nous reprenons dans le schéma ci-dessous.

Tab. 3.1 – Modes d'exploitation existants

Mode d'exploitation	Solution Informatique		Compétences	
	Interne	Externe	Internes	Externes
Tout Interne	X		X	
Intermédiaire 1	X			X
Intermédiaire 2		X	X	
Tout Externe		X		X

Nous pouvons donc distinguer quatre modes d'exploitation.

Le mode d'exploitation « Tout Interne » est le mode d'exploitation traditionnel : pour mettre en place une solution informatique, on achète le matériel et le logiciel, et un ou plusieurs informaticiens employés par l'entreprise sont attachés à la gestion de la solution.

Le mode d'exploitation « Tout Externe » est le cas d'une entreprise désirant déployer une application qui demande des ressources matérielles et des compétences qu'elle ne possède pas en interne. Elle peut alors décider de faire appel à une société externe pour gérer la solution.

Le mode d'exploitation « Intermédiaire 1 » est le cas d'une entreprise qui désire avoir la solution informatique en interne, mais qui n'a pas les compétences pour gérer cette solution. La solution sera donc déployée dans l'entreprise, mais sa gestion sera assurée par un prestataire externe.

Finalement, le mode d'exploitation « Intermédiaire 2 » est le cas d'une entreprise qui désire gérer la solution informatique, mais qui n'a pas spécialement les moyens de la déployer sur son site pour diverses raisons (salle informatique non disponible, ...).

1.2 Affinement de la première classification

La classification que nous venons de proposer nous semble intéressante. Dans un souci de précision, il paraît pertinent d'affiner davantage cette typologie selon la façon dont l'entreprise va acquérir le logiciel et le matériel ou en d'autres mots, selon le type d'acquisition.

Le logiciel peut s'obtenir par différents biais : il peut être développé, acheté ou loué. S'il est acheté (plusieurs types d'achat de licences), il peut l'être avec ou sans le matériel nécessaire à son utilisation. Le matériel, lorsqu'il n'est pas fourni avec le logiciel, peut être soit acheté soit loué. Par rapport à l'éventuelle location, notons que la location de logiciel s'inscrit dans le cadre d'un accès de l'application à distance. C'est une notion de 1-to-many ; c'est à dire que pour une seule et même application, il y aura plusieurs clients. C'est le cas de l'Application Service Provider. Lorsqu'une application est louée, on y accède à distance. Le

développement en interne va aboutir à une application qui sera gérée par l'entreprise elle-même. La solution finale pourra être en interne ou en externe.

Voici un schéma intégrant les différentes possibilités d'acquisition de logiciel pour chaque mode d'exploitation :

Tab 3.2 – Type d'acquisition de logiciel en fonction du Mode d'Exploitation

Mode d'exploitation	Software		
	Développement Interne	Achat	Location
Tout Interne	X	X	
Intermédiaire 1		X	
Intermédiaire 2	X	X	
Tout Externe		X	X

Comme on vient de l'expliquer, si le mode d'exploitation choisi est Tout Interne, alors le logiciel sera soit développé en interne, soit acheté. Dans le mode d'exploitation Intermédiaire 1, il n'est pas possible pour l'entreprise de développer son propre logiciel, mais elle ne peut pas non plus le louer car les machines sont en interne. Il ne lui reste comme possibilité que l'achat. Une entreprise qui veut externaliser la localisation de la solution mais qui désire la gérer (mode d'exploitation Intermédiaire 2) peut soit développer le logiciel elle-même soit l'acheter. Finalement, dans le mode d'exploitation Tout Externe, l'entreprise devra accéder à l'application à distance. Elle peut donc acheter le logiciel ou le louer.

Pour finir l'étude des modes d'exploitation, nous pouvons faire une distinction sur la façon dont le logiciel sera acheté. Il pourra l'être sur mesure ou existant (acheté tel quel ou légèrement modulable), et il pourra également inclure le matériel nécessaire à son utilisation.

Nous arrivons finalement à une classification des modes d'exploitation :

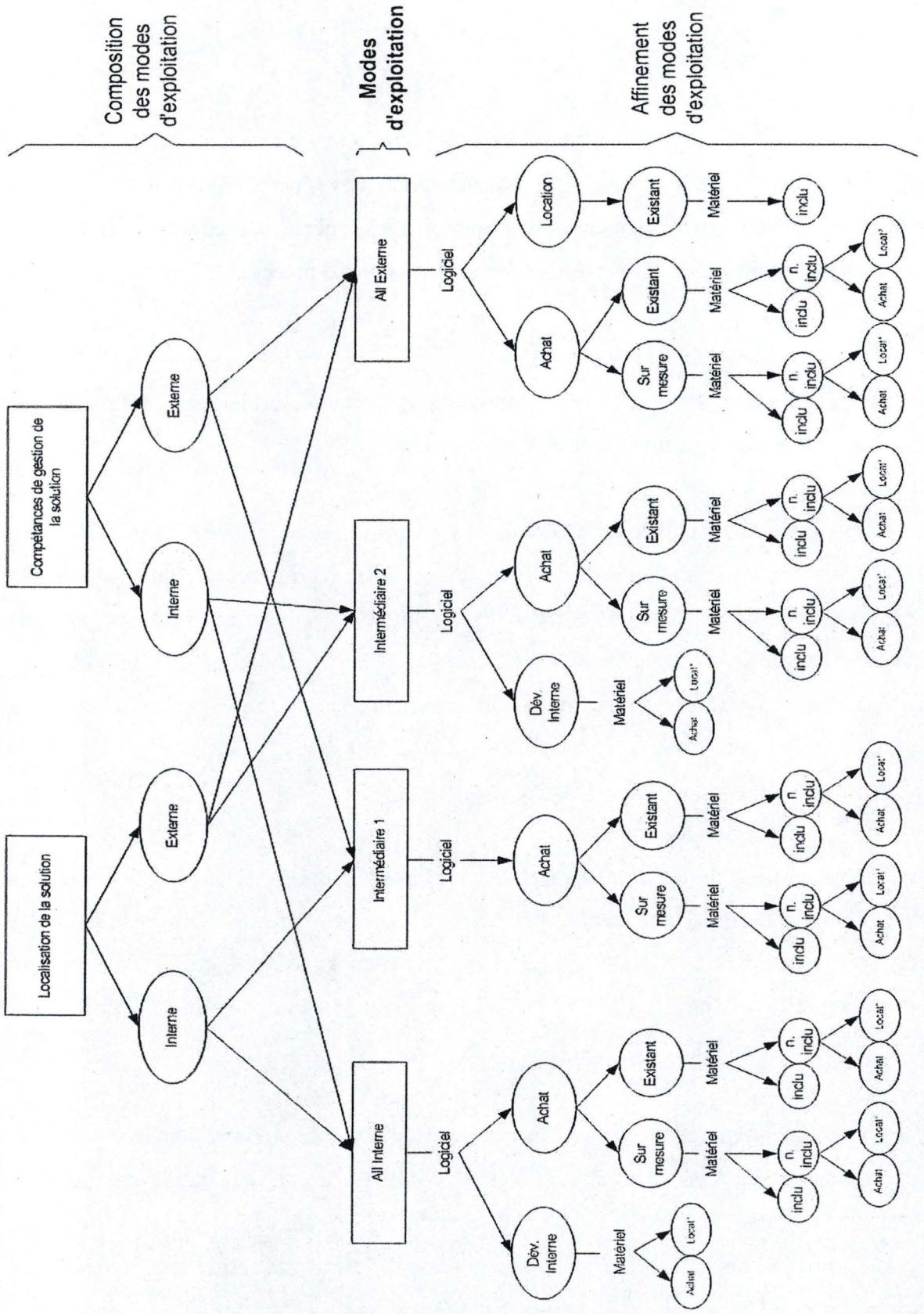

Fig 3.1 – Modes d'Exploitation : détail

1.3 Housing

a) Introduction

Après avoir défini précisément ce que nous entendons par « housing », nous donnerons ensuite, en nous basant sur nos recherches, les caractéristiques générales des offres de housing existantes. Nous tenterons finalement de faire ressortir les aspects de sécurité liés au housing à travers la sécurité physique des serveurs et de la gestion des données.

b) Définition

Nous venons de voir qu'il existe quatre modes d'exploitation principaux, définis par la localisation de la solution informatique et des compétences.

Lorsque la solution est déployée à l'extérieur de l'entreprise, deux cas de figures peuvent se présenter : soit le matériel est fourni avec le logiciel, soit il ne l'est pas. Une des possibilités est alors de louer un serveur capable d'accueillir la solution dans une infrastructure sécurisée : cette étape est appelée le « Housing ». Le Housing porte sur l'installation de n'importe quel logiciel. Le Housing est donc la location d'un serveur dans une infrastructure sécurisée, à laquelle en principe seul le locataire a accès.

c) Recherches

Nos recherches portent sur les offres de Housing au Luxembourg. Le détail de ces recherches se trouve dans l'annexe A. Les renseignements que l'on trouve en premier sont la taille des disques durs (entre 4 et 80 GB), le transfert limite par mois (entre 4 et 30 GB), les prix d'initialisation et le prix mensuel (de 50 à 2500 euros pour le premier, et de 35 à 1100 euros pour le second).

Nous pensons que d'autres éléments d'importance équivalente à ceux évoqués ci-dessus méritent d'être pris en considération dans l'analyse d'une offre de housing. Nous pensons notamment à la vitesse de la bande passante du serveur, à la garantie de cette bande passante, à la garantie de l'uptime du serveur, à la signalisation de la localisation géographique du serveur, ou encore à la durée de préavis lors de la rupture du contrat et au type de support offert au client.

Ainsi, nous fûmes surpris de constater que parmi les offres de housing que nous avons analysées (à l'aide de la grille de questions figurant en annexe), aucun fournisseur n'a donné la capacité de la bande passante du serveur. La moitié se donnent le droit de casser le contrat sans durée de préavis, mais presque tous garantissent un uptime de 99.9% ou de 99.99%. La plupart signalent l'emplacement géographique des serveurs, et fournissent un support après vente, au minimum par email.

d) Housing et sécurité

Dans cette partie nous allons expliquer quels sont les aspects de sécurité liés à l'infrastructure nécessaire pour déployer une solution informatique. Notre intention n'est pas de faire une description détaillée voire exhaustive des aspects de sécurité liés au housing, mais bien d'attirer l'attention du lecteur sur ces principaux aspects. Dans cette perspective, nous aborderons successivement la sécurité physique des serveurs, la protection des données, et la gestion des back-ups. Nous envisagerons également l'utilité de la technologie RAID (acronyme de *Redundant Array of Independent Disks*).

Sécurité physique des serveurs

La sécurité physique concerne tout ce qui est installé avant l'utilisation proprement dite de l'ordinateur : alarmes, clefs, caméras... La sécurité physique est l'une des formes de sécurité la plus fréquemment oubliée. Sur ce plan, la première chose à faire est un plan définissant tout les besoins de sécurité. Dans l'absolu, il faut également avoir une liste de questions, du type "qui a un accès à mon serveur"... Afin d'être capable de réagir rapidement en cas de sinistres, il importe également d'avoir un plan expliquant la façon de récupérer des données perdues. [Ga02]

Assurer la protection des ordinateurs requiert du matériel dont la qualité ne peut être négligée. En effet, en cas de sinistre, la subsistance du business peut dépendre des mesures de sécurité qui ont été prises et de la qualité du matériel choisi pour ce faire. Premièrement, il faut un environnement adéquat pour les machines, c'est-à-dire un environnement qui protège le matériel contre toutes sortes de sinistres. Passons brièvement en revue les principaux sinistres contre lesquels il s'agit de se prémunir.

- Feu : s'assurer qu'il y a un équipement extincteur à proximité.
- Fumée : ne jamais fumer dans la salle des ordinateurs et installer des détecteurs de fumée.

- Poussière : Maintenir la salle des ordinateurs avec le minimum de poussière possible.
- Tremblement de terre : Ce type de catastrophe n'est pas improbable. Il faut veiller à placer les ordinateurs dans une salle sans risque.
- Explosion : Pour que le business puisse continuer, il faut que les backups soient hors-site.
- Température extrêmes : éviter que les ordinateurs ne soient trop chauds ou trop froids.
- Humidité : le taux optimal est de 20% ; il faut veiller à ne pas monter trop haut.
- Eau : monter une sonde d'eau tout près l'ordinateur.

[Ga02]

Comme la salle informatique contient toutes les données vitales de l'entreprise, il faut éviter à tout prix qu'une personne mal intentionnée ne puisse s'y infiltrer. Il faut donc faire attention aux planchers surélevés, aux faux plafonds, aux conduites d'airs,... Le vandalisme frappe partout, y compris dans les salles informatiques. Gardons cela en tête. Pour empêcher le vol de matériel (vol de RAM par exemple). Il est important également de fixer physiquement les ordinateurs. Il convient aussi de prendre des mesures protectrices particulières pour les ordinateurs portables.
Au-delà de la sécurité du matériel, une attention particulière doit être portée aux données.

Protection des données

L'écoute clandestine est probablement le type de perte de données le plus difficile à détecter et celui dont les dégâts sont les plus lourds. Il y a beaucoup de types, mais il importe de savoir que les réseaux sans-fil 802.11 ne sont pas du tout sécurisés. Il devient dès lors facile d'écouter les données, et la protection est faible. Il faut donc, dans une perspective préventive, chiffrer les données pour les rendre inutilisables.

Gestion des backups

Les backups vont de l'enregistrement d'un document sur une disquette à la copie de tout un système sur un support de bandes magnétiques de plusieurs dizaines de gigas, capable de restaurer tout le système. On n'insistera jamais assez sur l'utilité de faire des backups : on peut toujours racheter un nouveau processeur et un nouveau disque dur, mais les données perdues ne peuvent, quant à elles, être rachetées... Et rien ne peut prévoir leur disparition. Il s'agit donc d'être extrêmement prudent à leur égard... [Ga02]

Il ne faut jamais oublier que les backups contiennent toutes les données de l'entreprise. Quiconque a la possession des bandes a par conséquent accès à toutes les données contenues sur ces bandes. Pour cette raison, il est nécessaire de protéger les backups autant que les ordinateurs eux-mêmes. Quelques protections supplémentaires sont à prendre en compte, comme les buffers d'une imprimante, ceux d'un scanner, ou la RAM d'un terminal X. [Ga02]

Lorsqu'une entreprise décide de faire un backup, il s'agit au préalable de répondre à la question suivante : que doit-on sauvegarder ? Il y a à cette question deux réponses correspondant à deux approches différentes : sauvegarder soit tout ce qui ne peut pas être perdu, soit tout le système afin de pouvoir le restaurer rapidement en cas de nécessité. La seconde approche peut paraître coûteuse, mais le coût de CD's ou de Dvd's est maintenant très faible. Quatre types de backups existent :

- Level-zero backup: copie du système original.
- Full backup: sauvegarde de chaque fichier du système.
- Incremental backup: sauvegarde des fichiers qui ne l'ont pas encore été.
- Combination : full backup et ensuite incremental.

[Ga02]

La durée de vie d'un backup est également aléatoire; certains fichiers peuvent être supprimés après un mois, tandis que des fichiers tels des comptes annuels doivent être gardés « pour toujours ». Il y a quelques règles à appliquer pour les backups : ne pas les laisser près des ordinateurs (en cas de désastre), les enregistrer en lecture seule, afin qu'ils ne soient pas effacés accidentellement, et les protéger avec des mots de passe qui ne pourront jamais être retrouvés. De plus, les backups sont souvent utilisés dans les poursuites judiciaires. Si l'entreprise décide de supprimer tous ses documents, les mêmes règles doivent être appliquées aux backups. [Ga02]

En outre, afin de garantir au mieux la disponibilité de l'application, il est important de s'assurer de la redondance des données. Au niveau des disques, cette redondance peut se faire par exemple via la technologie RAID Au-delà du backup proprement dit, il y a aussi une redondance des données au niveau des disques qui peut être effectuée, via la technologie RAID.

RAID

La technologie RAID (acronyme de *Redundant Array of Independent Disks)*, permet de constituer une unité de stockage à partir de plusieurs disques durs. L'unité ainsi créée (appelée grappe) a donc une grande tolérance aux pannes (haute disponibilité), ou bien une plus grande capacité/vitesse d'écriture. La répartition des données sur plusieurs disques durs permet donc d'en augmenter la sécurité et de fiabiliser les services associés. Nous allons citer les différents types de technologies RAID, et décrire plus en détails les plus utilisés. [Pi04]

Cette technologie a été mise au point en 1987 par trois chercheurs (*Patterson, Gibson* et *Katz*) à l'Université de Californie (Berkeley). Depuis 1992 c'est le RAID Advisory Board qui gère ces spécifications. Elle consiste à constituer un disque de grosse capacité à l'aide de plus petits disques. [Pi04]

Les disques assemblés selon la technologie RAID peuvent être utilisés de différentes façons, appelées Niveaux RAID. L'Université de Californie en a défini 5, auxquels le niveau 0 est venu s'ajouter. Chacun d'entre eux décrit la manière par laquelle les données sont réparties sur les disques:

- Niveau 0: appelé striping
- Niveau 1: appelé mirroring, shadowing ou duplexing
- Niveau 2: appelé striping with parity (obsolète)
- Niveau 3: appelé disk array with bit-interleaved data
- Niveau 4: appelé disk array with block-interleaved data
- Niveau 5: appelé disk array with block-interleaved distributed parity

Chacun de ces niveaux constitue un mode d'utilisation de la grappe, en fonction:

- des performances
- du coût
- des accès disques

Les solutions RAID généralement retenues sont le RAID de niveau 1 et le RAID de niveau 5.

Le choix d'une solution RAID est lié à trois critères :

- **la sécurité** : RAID 1 et 5 offrent tous les deux un niveau de sécurité élevé. Toutefois, la méthode de reconstruction des disques varie entre les deux solutions. En cas de panne du système, RAID 5 reconstruit le disque manquant à partir des informations stockées sur les autres disques, tandis que RAID 1 opère une copie disque à disque.
- **Les performances** : RAID 1 offre de meilleures performances que RAID 5 en lecture, mais souffre lors d'importantes opérations d'écriture.
- **Le coût** : le coût est directement lié à la capacité de stockage devant être mise en oeuvre pour avoir une certaine capacité effective. La solution RAID 5 offre un volume utile représentant 80 à 90% du volume alloué. La solution RAID 1 n'offre par contre qu'un volume disponible représentant 50 % du volume total (étant donné que les informations sont dupliquées). [Pi04]

Le housing propose donc de louer un serveur capable d'accueillir la solution dans une infrastructure sécurisée. Une entreprise peut désirer déployer en interne la même infrastructure. Nous voulons attirer l'attention du lecteur sur le fait que le déploiement interne d'une solution informatique sécurisée nécessite une infrastructure dont la gestion est relativement lourde. La construction et la gestion de cette infrastructure impliquent des frais importants. Nous avons décidé de ne pas donner de prix car la littérature manque de chiffre précis, mais il est admis par les professionnels de la sécurité que la mise en œuvre d'une telle infrastructure implique des coût supportables uniquement pour des entreprises de grande taille.

Nous venons de définir ce que sont les modes d'exploitation. Il sont au nombre de quatre, et sont caractérisés par la localisation géographique de la solution (à l'intérieur de l'entreprise, ou à l'extérieur) et par la disponibilité des compétences nécessaires à la gestion de cette solution. Nous avons aussi essayé de montrer les aspects de sécurité liés à l'hébergement d'une salle informatique. Comme décrit dans la méthodologie générale, nous allons maintenant analyser chaque composant de l'architecture en fonction de son mode d'exploitation, en tentant de l'isoler le plus possible des autres composants.

Chapitre 2 : Architectures e-business : définition des composants et étude indépendante de leurs aspects de sécurité en fonction du mode d'exploitation.

2.1 Introduction

Dans ce chapitre, nous allons dans un premier temps donner une définition des composants des architectures e-business que nous avions évoqués dans notre partie théorique. Ensuite, nous citerons les principaux aspects de sécurité liés à chaque composant. En se basant sur les recherches que nous avons faites (voir annexes), nous caractériserons les composants en fonction de leur mode d'exploitation principalement au niveau de la sécurité d'une part, mais également sur d'autres critères, tels que le coût, les caractéristiques techniques du composant, etc.

Les architectures sur lesquelles nous allons travailler sont le résultat de recherches faites par V. Rosener sur le projet Acces-PME. Avant de détailler chaque composant, nous allons expliquer ces architectures.

2.2 Les architectures e-business

Le résultat de V. Rosener [Ro04] est la définition de deux architectures différentes, expliquées par les diagrammes de composant [Fig 3.2] et [Fig 3.3]. Ces diagrammes définissent les composants minimaux indispensables à toute forme d'architecture e-business. Nous allons définir les composants de ces deux diagrammes.

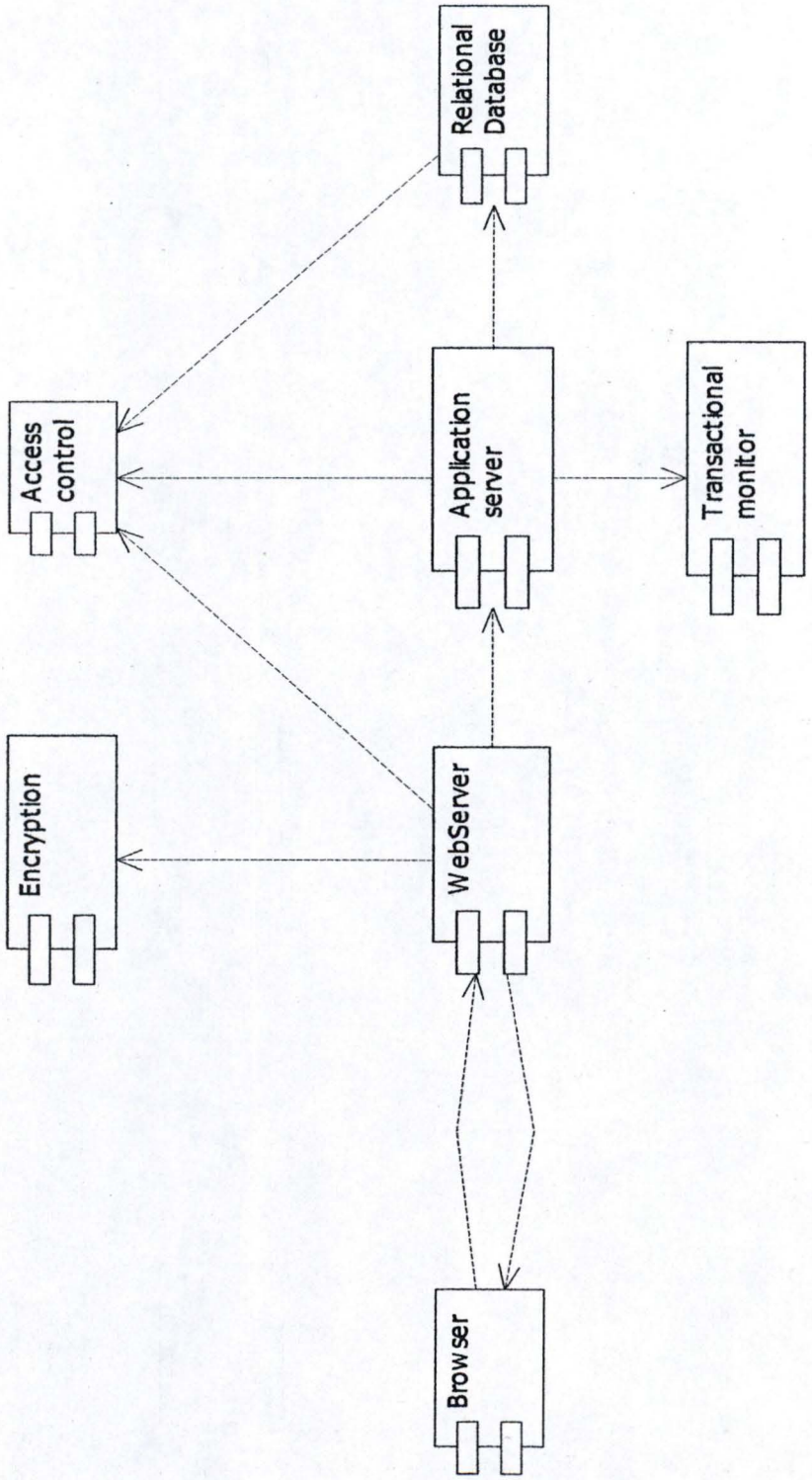

Fig 3.2 - Architecture avec Application Server

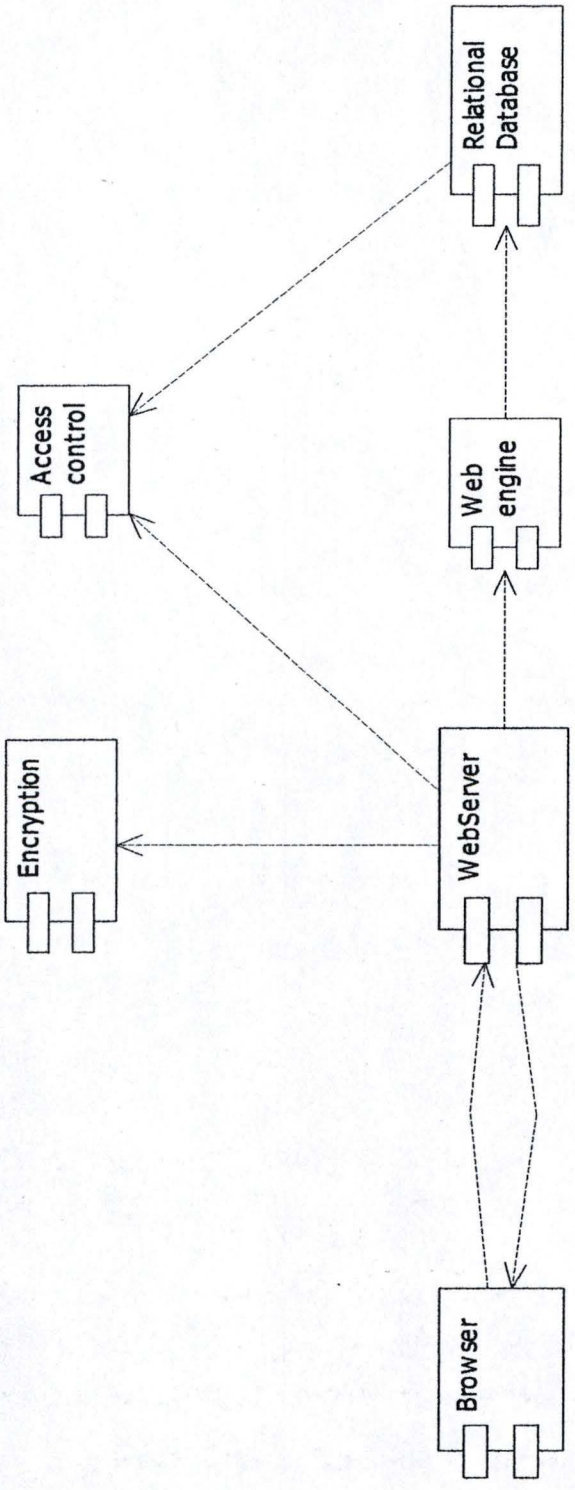

Fig 3.3 - Architecture avec Web Engine

Nous avons donc deux architectures Web qui se différencient l'une de l'autre par l'utilisation soit d'un Application Server, soit d'un Web Engine. Nous définirons les composants de ces deux diagrammes dans un instant, mais il importe de souligner que la seule différence entre ces deux architectures repose sur l'utilisation de l'un ou de l'autre. Ce choix doit être fait par un spécialiste du design, et ne nous concerne pas à ce niveau-ci d'analyse de la sécurité. Par conséquent nous n'allons considérer qu'une seule architecture, pouvant comporter soit un Application Server, soit un Web Engine.

2.3 Définitions des composants

Comme annoncé ci-dessus, avant de faire l'étude de la sécurité de chaque composant en fonction de son mode d'exploitation, nous allons proposer une brève définition de chacun des composants repris dans les schémas. Une remarque s'impose : les termes que nous allons aborder n'ont pas de définition univoque. Selon l'auteur ou la source, l'acceptation du concept diffère. Dans le cadre de ce travail, nous avons choisi de nous rallier aux acceptations de l'équipe du CRPHT.

2.3.1 Web Server

Dans nos recherches, nous avons trouvé plusieurs significations pour le terme « serveur Web ». Parfois il désigne le logiciel, parfois le matériel, et d'autres fois il concerne les deux réunis. Nous supposerons dans ce document que le serveur Web est purement logiciel.

Un serveur Web est donc un logiciel qui reçoit des requêtes http et les interprètes. Si la requête du browser est statique (.htm, .html, ou un document directement accessible) il fournit alors la page ou le document demandé. Si la requête est dynamique (php, jsp, asp...) il transfère alors la requête au *Web Engine* ou à l'*Application Server* qui se chargera de générer du code html et de le renvoyer au serveur Web. Le serveur Web doit finalement transférer ce code au client qui a fait la requête.

2.3.2 Application Server et Web Engine

La définition des termes « Application Server » et « Web Engine » demande plus que quelques lignes. Nous allons d'abord donner une définition de ces deux éléments, ensuite, dans une perspective comparative, nous en donnerons quelques points communs et différences.

Sur le marché, on appelle bien souvent « Application Server » la combinaison de trois choses : un Web Serveur, un Application Serveur proprement dit (ce que nous appellerons application serveur) et un environnement de développement. Certains Application Server incluent une Base de Données. Parfois ce qui est appelé « Application Server » sur Internet n'est en fait qu'un langage de pages dynamiques dans lequel une partie de programmation permet de traiter des informations.

Dans l'acceptation restreinte qui est la nôtre, l'Application Server réalise un ensemble de traitements en fonction de ce qu'il reçoit du Web Server. Il gère le « Business Logic », c'est à dire tout le traitement de l'information spécifique à l'exécution d'un processus de l'entreprise. Il comprend des « Business Component », qui encapsulent chacun une partie du Business Logic. Il inclut également le transactional monitor, que nous définirons ci-dessous. Il prend place dans une architecture 3-tiers, entre la couche présentation et le système de persistance de données.

Ce que nous avons appelé « Web Engine » au sein du projet Acces-PME recouvre l'ensemble des interpréteurs de scripts que l'on trouve du côté serveur dans une architecture e-business. Ces interpréteurs sont principalement PHP, ASP, JSP, CGI et Macromedia ColdFusion. Le Web Engine trouve lui aussi sa place dans une architecture 3-tiers, entre la représentation des données et le système de persistance de données. Il reçoit des requêtes du Web Server, exécute le scénario décrit et renvoie le code html généré au Web Server. Il est capable d'effectuer le code écrit dans le langage de script et de faire des accès à la Base de Données. Ce code peut être, entre autres, C, C++, java, Visual Basic, VBScript, JScript, Perl, PHP, Fortran, ou AppleScript. [Wr04]

Il existe de nombreuses similitudes entre les deux composants. Ils sont logiciels et font partie d'une logique 3-tiers, entre la partie GUI et le système de persistance de données. Leur rôle est de recevoir des informations en provenance du Web Server, de réaliser un certain nombre de traitements, et en fonction de l'état de l'environnement, de produire une réponse (le plus souvent sous la forme de code html) au Web Server. Ils peuvent tous les deux interagir avec le système de persistance de données, et peuvent être programmés dans différents langages de programmation. Au niveau du coût, le Web Engine et l'Application Server peuvent être trouvés en Open Source, et fournir de bonnes performances. Des solutions propriétaires existent aussi, mais ce qui est le plus coûteux est la partie de personnalisation du traitement de l'information pour l'Application Server ou le Web Engine. [Se01], [VR01], [Dr02]

Bien qu'ils présentent des caractéristiques communes, il y a des différences. L'Application Server est orienté « Business Component » : « bean » pour java et « COM » pour Microsoft. Il inclut un transactional monitor, permet un déploiement dynamique, et possède un Message Oriented Middleware[1]. On ne retrouve pas ces éléments au niveau du Web Engine, bien qu'ils permettent d'effectuer un certain nombre d'opérations qui auront été programmées. Au niveau de la puissance de calcul, l'Application Server permet de répondre à beaucoup plus de requêtes qu'un Web Engine. Le Web Engine n'est en général pas conçu pour traiter des millions de requêtes quotidiennement, alors que l'Application Server est spécialement utilisé pour recevoir une charge de travail très lourde. L'Application Server intègre un Transaction Manager qu'on ne retrouve pas au niveau du Web Engine, ce dernier restant centré sur des traitements simples. [Se01], [VR01], [Dr02]

Transactional monitor

Un moniteur transactionnel est un programme qui surveille une transaction pendant qu'elle passe d'une étape d'un processus à une autre. Le but du moniteur est de s'assurer que les transactions s'effectuent complètement ou, si une erreur se produit, de prendre des mesures appropriées. Les moniteurs de TP sont particulièrement importants dans les architectures trois-tiers qui fonctionnent en load-balancing, parce qu'une transaction peut être forwardée à différents serveurs. Concrètement, beaucoup de moniteurs transactionnels gèrent tout le load-

[1] MOM est une partie spécifique d'un middleware qui supporte l'échange de messages dans un environnement distribué. Les données sont échangées par message passing et/ou message queuing supportant des interactions synchrones et asynchrones entre les processus distribués. [Web14]

balancing des opérations, envoyant les différentes transactions aux serveurs les moins chargés. [Un01]

Nous voyons qu'il apparaît comme un composant indépendant sur le diagramme de composants de l'architecture, car il doit pouvoir conclure ou annuler une transaction complète (ACIDité), même en cas d'instabilité des autres composants. Cependant étant donné que le moniteur transactionnel est inclus dans l'Application Server, nous n'allons pas davantage le détailler.

2.3.3 Relational Database

Le composant Relational Database correspond à la Base de Données de l'architecture.

2.3.4 Access Control

Dans ce cadre-ci, le contrôle d'accès correspond au contrôle d'accès de l'utilisateur de l'architecture e-business qui va vouloir accéder à une ressource.

2.3.5 Encryption

Le composant encryption se charge du chiffrement et du déchiffrement des communications sécurisées.

2.3.6 Browser

Le browser est le navigateur client. Etant donné que ce composant n'est pas analysé dans le cadre de cette étude, nous n'en dirons pas davantage.

Ayant défini tous les éléments de l'architecture et les modes d'exploitations possibles, nous pouvons maintenant étudier chaque composant de l'architecture en fonction de ses modes d'exploitation.

2.4 Etude des aspects de sécurité des composants en fonction du mode d'exploitation

Maintenant que nous avons défini chaque composant, nous allons les étudier. Cette étude se fera le plus indépendamment possible des autres composants. La structure de cette section est la suivante : nous dressons un portrait de la sécurité le concernant, suivi par une analyse des aspects de sécurité du composant en fonction de son mode d'exploitation, en nous basant sur les recherches que nous avons menées.

2.4.1 Web Server

a) Introduction

Nous allons commencer par faire quelques commentaires relatifs à la sécurité du serveur Web, et présenterons les étapes importantes dans le processus de sécurisation. Nous verrons que la présence d'options « telles quelles » peut comporter des faiblesses, et nous en présenterons trois. Comme pour le housing, nous ne voulons pas faire une étude détaillée de la sécurité d'un serveur Web, mais bien éveiller le lecteur aux problèmes potentiels de sécurité qui y sont liés. Ensuite nous aborderons brièvement les caractéristiques générales des serveurs Web que nous avons recensés dans nos recherches. Enfin, nous envisagerons les aspects de sécurité liés aux modes d'exploitation tels que nous les avons présentés dans le chapitre précédent.

b) Sécurité

Le serveur Web est l'interface qui va directement interagir avec l'utilisateur. C'est le premier élément de l'architecture qui va être touché par une attaque externe. Il est communément admis que chaque service d'un serveur apporte un certain nombre de menaces. Au niveau du serveur Web pour une PME, certaines options par défaut ne sont pas nécessaires. Nous retiendrons qu'il vaut mieux garder une architecture offrant un minimum de services. [Gh99]

L'exploitation sécurisée d'un serveur Web passe par un certain nombre d'étapes, que nous allons détailler. Nous rappelons que nous ne cherchons pas à être exhaustifs dans la liste des étapes ; notre intention est de montrer les principaux éléments de sécurité liés à un serveur Web.

Après l'installation proprement dite, la première étape de la configuration du serveur est la création d'un utilisateur root, ou superutilisateur. Cet utilisateur aura les droits absolus sur le serveur : création ou suppression de fichiers, création d'utilisateurs ou de groupes d'utilisateurs, création d'administrateurs, ... La gestion de toutes les permissions du serveur dépendent de ce choix. La politique de sécurité de l'entreprise devra évaluer le choix de ce superutilisateur et l'approuver, pour s'assurer que la décision prise sera optimale pour la sécurité de l'entreprise. [Gh99]

La deuxième étape de la configuration consistera à l'établissement des permissions d'accès à certains fichiers sensibles. Les documents se trouvant dans le répertoire root du serveur nécessitent une précaution particulière : se sont les fichiers de configuration, de log, de traitements de l'information, les fichiers administrateurs etc. [Gh99]

Une troisième étape de cette configuration est d'attribuer correctement les droits aux différents processus et routines du serveur. Le problème vient du fait que pour pouvoir écouter sur les ports réseaux entre 0 et 1023 (les ports indispensables au bon fonctionnement du serveur), ce dernier doit avoir les droits administrateurs. Mais dans son exécution, le serveur crée des processus fils qui vont traiter les routines nécessaires à son bon fonctionnement. Une erreur de configuration qui donnerait aux fils les mêmes droits que le processus père poserait des problèmes potentiels. Comme nous l'avons dit, « less is better ». Il y aura théoriquement un processus présentant d'avantage de failles qu'un autre, et les attaques se tourneront donc vers celui-ci. Cette option d'héritage de privilèges est défini par défaut sur la plupart des serveurs Web, et doit par conséquent faire l'objet d'une attention particulière. [Gh99]

Au-delà de la configuration proprement dite, il faut prendre garde à certaines propriétés inhérentes au monde informatique. Comme pour tous les logiciels, les serveurs Web sont délivrés avec des options sélectionnées par défaut. Un exemple classique de ces options gênantes est le cas d'un répertoire ne contenant pas de fichier « index.html ». Dans ce cas certains serveurs Web renvoient au client un listing de tous les fichiers et dossiers existants dans le répertoire pointé par l'adresse. Une conséquence de cela est qu'un utilisateur malveillant pourrait par exemple s'accaparer les fichiers des sources des scripts s'exécutant sur le serveur pour les analyser et ainsi organiser une attaque.

Une autre option présente sur certains serveurs est le « server-side includes », ou le SSI, qui offre la possibilité d'inclure une commande dans un fichier html. Les commandes du fichier sont alors exécutées avec les droits du serveur. Il suffit dès lors pour un pirate de réussir à placer un fichier dans un répertoire, pour ensuite pointer son navigateur dessus, et exécuter une commande arbitraire. A nouveau, cette option offre des fonctionnalités étendues, mais provoque de nouvelles failles de sécurité. Une dernière option par défaut pouvant provoquer des problèmes est celle des liens symboliques. Ils comportent leur dose de menaces, car les administrateurs n'ont pas toujours le contrôle sur tous les liens, et de nouveaux liens peuvent être crées, pointant, par exemple, sur les fichiers CGI (traitement de l'information). [Gh99]

En résumé nous voyons qu'il existe de nombreux problèmes potentiels autour de l'utilisation d'un serveur Web. Il existe des lignes de conduites et des bonnes pratiques pour en éviter le maximum, mais l'installation, la configuration, et la maintenance d'un serveur Web servant de noyau à une architecture e-business doit rester le travail d'un professionnel.

c) Recherches

Après ces quelques considérations générales sur les aspects de sécurité liés au serveur Web, nous allons passer en revue les besoins matériels nécessaires pour le faire fonctionner.

Dans nos recherches sur les serveurs Web (voir Annexe B pour plus de détails), nous avons trouvé énormément de solutions. De nombreuses caractéristiques les différencient les unes des autres : le prix (libre ou propriétaire), la gestion à distance (possible ou non), le nombre de clients simultanés, le temps de réponse moyen, la possibilité d'utiliser SSL, l'OS sur lequel on l'installe ...

Le matériel requis pour faire fonctionner un serveur Web peut être aussi basique qu'un ordinateur personnel. Le serveur le plus utilisé, Apache, requiert 32 MB de RAM et 12 MB de disque dur pour son fonctionnement. L'IIS de Microsoft demande plus de ressources : 256 MB de RAM et plus de 2 GB de disque dur. En fait, un simple 486 suffit pour certains usages que l'on voudrait faire d'un serveur Web. Mais lorsqu'un grand nombre d'utilisateurs doivent se connecter en même temps sur le serveur, il faut alors du matériel spécialisé. L'utilisation de matériel est aussi justifié pour d'autres raisons de sécurité : redondance du matériel, fermeture à clé de la machine, ... Il existe du matériel spécialement construit pour supporter un serveur Web à partir de 300 euros.

d) Modes d'Exploitation

Maintenant que nous avons défini de manière détaillée ce que nous entendons par Web Server, que nous en connaissons les principales caractéristiques de sécurité, nous pouvons étudier la sécurité d'un serveur Web en fonction de son mode d'exploitation.

Tout Interne

Il est possible pour quelqu'un sans compétence pointue de faire une page Internet en utilisant un éditeur de texte wysiwyg, puis d'installer le logiciel sur son ordinateur personnel qui serait relié à Internet. Pour une telle utilisation, le logiciel doit être simple d'utilisation et d'administration ; Apache est un contre-exemple de simplicité, car son utilisation requiert des compétences particulières.

Le coût du déploiement et de l'exploitation de ce genre de serveur Web est évidemment très faible : un ordinateur personnel, une connexion à Internet, et le logiciel qui peut être gratuit. Cependant, le budget est inversement proportionnel au niveau de sécurité : il n'y a pas de back up automatique des données, la disponibilité est faible (l'ADSL classique est lente à l'upload, et le serveur n'est pas conçu pour recevoir une masse de connexions simultanées), et le logiciel peut être peu robuste aux attaques. Le niveau de sécurité global n'est pas suffisant pour faire de l'e-commerce. Nous avons vu dans la partie « sécurité » du Web Server que beaucoup de manipulations délicates sont nécessaires à la bonne mise en œuvre du déploiement d'un serveur, et il nous semble primordial que ces manipulations restent dans le domaine des spécialistes.

Pour le type d'e-business défini dans ce document, nous pouvons conclure en disant que ce mode d'exploitation n'est pas possible.

Tout Externe

Deux sous-modes d'exploitation existent pour le Web Server : la location et l'achat.

Pour la location, le critère principal qui différencie les solutions existantes est le fait que le serveur soit dédié ou non. Un hébergement sur un serveur partagé est intéressant si le site doit être disponible rapidement, que le budget est limité, et que l'espace disque nécessaire est

faible (en général, inférieur à 100 MB). Un hébergement sur un serveur dédié est avantageux quand le site est complexe et dynamique, que les pics de trafic peuvent être importants, que l'espace disque nécessaire est de l'ordre de plusieurs gigas, ou que des options de sécurité doivent être mises en place (firewall, VPN...)

Il existe au Luxembourg des hébergements avec serveur dédié dont les prix varient d'une centaine d'euros à 500 euros par mois. Le prix de la location d'un serveur non-dédié au Luxembourg varie de 5 à 80 euros par mois.

Les points importants à retrouver chez un fournisseur sont le volume de transfert par mois (limité ou non ; quelle limite, possibilité d'étendre le volume en cas de dépassement), le volume disponible sur le serveur, la redondance des données, un uptime garanti, et le fait de pouvoir connaître l'emplacement géographique du serveur.

Dans nos recherches, nous n'avons pas trouvé de fournisseur qui garantisse une bande passante minimale pour le serveur, et nous n'avons trouvé chez aucun un nombre limite d'utilisateurs simultanés. Il est donc important de pouvoir évaluer cette charge soi-même, et de pouvoir tester la solution avant de l'acheter.

Le cas de l'achat du logiciel et de son installation sur un serveur en Housing est semblable à la location de logiciel avec serveur dédié, mis à part le fait que n'importe quel logiciel peut être installé, alors que dans le cas précédant le logiciel du Web Server est pré-installé. Cette solution est plus lourde financièrement, mais a l'avantage d'être plus personnalisable.

Intermédiaire 1

Décider d'avoir en interne son propre serveur Web sans l'administrer peut représenter une solution coûteuse : le matériel spécialisé, une connexion rapide, et un administrateur externe peuvent coûter cher. L'avantage principal de ce mode d'exploitation est que les fichiers contenus dans le Server sont en interne, et qu'ils ne circulent jamais en clair sur le réseau (étant donné que la gestion du contenu d'un serveur Web distant se fait souvent via le protocole ftp qui ne chiffre pas les données).

Pour des raisons de disponibilité, il faut investir au moins dans une ligne coûteuse de type SDSL, dans du matériel qui est spécialement conçu pour être un serveur Web, dans une

personne externe qui va s'assurer de la gestion de la solution, et dans des dispositifs de sécurité élémentaires : une pièce fermée, un détecteur de fumée, une redondance du système électrique…

Intermédiaire 2

Comme pour le cas All Interne, il est envisageable que la PME installe un Web Serveur qui est simple d'installation et d'administration. Il est donc possible pour la PME de louer un serveur en Housing, et d'installer ce serveur Web. Cependant un tel serveur ne sera jamais configuré pour avoir un niveau général de sécurité suffisant pour faire du commerce électronique.

Nous pensons donc que de tels serveurs simples d'administration ne conviennent pas pour tous les types d'e-business. Si de l'e-publishing ou de l'e-advertising restent possibles, la vente en ligne s'avère impossible.

Nous voyons donc que les deux modes d'exploitations sécurisés pour le serveur Web sont Tout Interne et Intermédiaire 1.

Après avoir parlé du serveur Web, nous allons maintenant aborder le composant Application Server.

2.4.2 Application Server

a) Introduction

L'Application Server est le composant logiciel qui gère toute la « Logique Métier » de l'entreprise. L'acquisition d'un Application Server est un investissement important généralement réservé aux entreprises de certaine taille. Il existe des Application Server en Open Source, mais cela ne représente que le framework dans lequel il faudra développer les applications propres à l'entreprise. Quel que soit le choix de l'Application Server, il faut garder à l'esprit qu'acquérir un Application Server représente un investissement non-négligeable.

L'application Serveur effectue un traitement de l'information personnalisé, complexe et massif. Si le traitement de l'information est basique, répétitif et non-personnalisé, alors un

traitement avec un langage de script peut être effectué. Malgré son coût élevé, une entreprise de petite taille qui nécessite un haut degré de sécurité, de concurrence d'accès aux ressources ou de traitement de l'information peut avoir intérêt à réaliser cet investissement.

Nous allons commencer par différencier les deux types d'Application Server existants. Ensuite, comme pour les deux premiers composants, nous allons expliquer les principales caractéristiques de sécurité liées à l'Application Server, pour terminer par l'étude de la sécurité du l'Application Server en fonction de son mode d'exploitation.

b) Etude

Les deux types d'Application Server existant sont le .NET de Microsoft et J2EE. En faire une comparaison est une tâche ardue. Etant donné qu'il s'agit d'une technologie changeante, les documents qui les comparent sont des articles sur Internet qui ne sont en général qu'un point de vue rarement neutre. Nous allons tenter de déceler les caractéristiques de chacun, et de peser globalement le pour et le contre.

Il est important de noter que J2EE est un standard, et que .NET est un produit. Ce standard est développé par Sun Microsystems et implémenté en java par des dizaines d'organisations – y compris Sun Microsystems lui-même. [AI03]

Tableau 3.3 – Comparaison des Application Server

Feature	**J2EE**	**.NET**
Type of technology	*Standard*	*Product*
Middleware Vendors	*30+*	*Microsoft*
Interpreter	*JRE*	*CLR*
Dynamic Web Pages	*JSP*	*ASP.NET*
Middle-Tier Components	*EJB*	*.NET Managed Components*
Database access	*JDBC SQL/J*	*ADO.NET*
SOAP, WSDL, UDDI	*Yes*	*Yes*
Implicit middleware(load-balancing, etc)	*Yes*	*Yes*

source : [VR01]

Arguments envers les deux plates-formes:

- Peu importe le choix de la plate-forme, les nouveaux développeurs devront être formés.
- Il est possible de développer des services Web avec les deux.
- Les deux plates-formes proposent entre autres des systèmes bon marché.
- Les deux plates-formes offrent une solution avec un vendeur unique.
- La « scalabilité » des deux solutions est théoriquement sans limite.

Arguments de .NET contre J2EE

- Les interfaces graphiques sont plus aisées avec .NET
- .NET propose des langages de programmation plus simple que java.
- .NET donne une neutralité du langage lorsque l'on développe une application e-business, alors que J2EE traite les langages différents comme des applications différentes.
- .NET est fortement lié et optimisé à l'OS sur lequel il repose.

Arguments de J2EE contre .NET

- J2EE est vendu par une industrie entière.
- J2EE est une plate-forme qui a fait ses preuves, alors que .NET repose sur une réécriture, ce qui introduit de nouveaux risques.
- Les services Web de .NET ne sont pas interopérables avec les standards de l'industrie. J2EE est adaptable sur le matériel existant.
- J2EE offre une neutralité du choix de la plate-forme. La portabilité est bonne (mais pas gratuite).
- J2EE inclut le Java Connector Architecture, qui a déjà fait ses preuves en terme d'intégration.
- J2EE peut être utilisé sur n'importe quel OS. Les développeurs peuvent choisir l'environnement dans lequel ils sont le plus à l'aise.
- A l'heure actuelle, le C# de Microsoft n'est pas encore aussi mature que Java.

[VR01]

c) Sécurité

En configurant avec grande précaution les éléments sensibles de l'architecture que nous avons vus (Base de Données et serveur Web), nous augmentons fortement le niveau de sécurité général. Cependant, même le site le mieux configuré peut avoir d'importants problèmes potentiels de sécurité, dus aux « Server Side Scripts », qui est le traitement de l'information du côté serveur. Les scripts « CGI » (Common Gateway Interface) sont des programmes exécutés côté serveur. La raison pour laquelle ils sont tellement dangereux est qu'ils peuvent exécuter n'importe quelle commande sur le serveur. Pour cette raison, même si le serveur Web et la Base de Données sont parfaitement configurés et sécurisés, cela ne suffit pas pour satisfaire un niveau de sécurité global. [Gh99]

Il existe deux façons de réduire le risque d'avoir des failles de sécurité dans un logiciel côté serveur : d'une part, le logiciel doit être conçu et implémenté avec des techniques qui minimisent les risques de problèmes de sécurité. D'autre part, des méthodes d'analyse peuvent être appliquées sur le logiciel pour tenter de déceler l'existence de structures dangereuses ou de comportements risqués sur le serveur. [Gh99]

Le problème de la conception non sécurisée de logiciel est imputable à plusieurs facteurs. Tout d'abord, les développeurs ne font pas spécialement attention aux risques potentiels de sécurité du logiciel qu'ils écrivent. Cela est dû en partie au fait que les délais pour concevoir un logiciel sont passés de 18 à 6 mois, et que dès lors les test du logiciel ne sont plus fait chez le développeur, mais directement chez le client, via des versions « Béta's ». Accepter des version beta's simplement à cause de leur gratuité doit être évité ! En effet, d'importantes failles de sécurité s'y retrouvent, et ne seront corrigées que plus tard. Ensuite le problème de la sécurité vient aussi du fait que les développeurs ne considèrent pas tous les aspects de sécurité lors du développement de leur logiciel, supposant que la sécurité est du domaine des analystes et des administrateurs. Ce point de vue n'est pas correct : c'est en effet tout le contraire. Les analystes et les administrateurs sont en général à la fin de la chaîne, et tentent de trouver les failles de sécurité. Le développement sécurisé d'un logiciel commence seulement à devenir un enjeu chez les développeurs. [Gh99]

Il existe des méthodes d'analyse du logiciel. Les développeurs produisent du code de ce qui doit être fait, et ne pensent que rarement à ce qui ne peut pas être fait avec le logiciel. Il importe que des tests portant sur autre chose que les spécifications du logiciel soient fait avant

la distribution du produit. Deux types de tests doivent être effectués sur un logiciel : les premiers pour s'assurer que le logiciel effectue correctement ce qu'on lui demande de faire, les seconds pour voir ce qu'il fait avec des inputs qui ne sont pas ceux attendus. Le but ici est de voir quelle sera la réaction du programme avec des données qui ne sont pas attendues. Il existe de nombreuses approches d'analyse de logiciel pour voir si des failles existent. On se réfère souvent à des analyses statiques ou dynamiques. [Gh99]

Les analyses statiques peuvent être manuelles ; c'est-à-dire qu'une personne autre que l'analyste ou le développeur va relire le code, pour voir s'il ne trouve pas de structures dangereuses. Pour illustrer l'analyse dynamique, nous allons prendre un exemple : dans le cas de serveurs Web, il est très dangereux de prendre comme paramètre d'un appel de fonction des arguments venant d'une requête http. L'analyse dynamique va chercher ce type d'appel dans le code. Un autre type de détection automatique porte par exemple sur la décomposition d'une action atomique. Par exemple, si une requête porte sur un document spécifique qui demande une authentification. Pendant la période d'authentification, si le document est remplacé par un autre, alors une personne malveillante pourrait obtenir accès à une partie du serveur qui ne lui est pas permise. Cette action doit être atomique, et des techniques d'analyse automatiques existent pour détecter le code qui n'y répond pas. [Gh99]

Nous venons d'expliquer les caractéristiques de sécurité des logiciels développés sur mesure pouvant effectuer un traitement de l'information du côté serveur. En nous basant sur cette analyse, nous pouvons détailler les modes d'exploitations possibles, et en donner les avantages et les inconvénients.

d) Application Server et Modes d'exploitation

Les Application Server sont basés sur des « Business Component » qui doivent être programmés pour l'entreprise. Avec tous les enjeux de sécurité que nous venons de voir, la PME n'a pas les compétences internes pour faire cette programmation, ni pour gérer l'Application Server. Les modes d'exploitations sont donc les suivants : Intermédiaire 1 ou All Externe. A nouveau, comme pour la Base de Données et le Web Server, installer un Application Server en interne demande une infrastructure particulière. La gestion de la sécurité peut demander beaucoup d'énergie pour une seule machine, et donc être très coûteux.

L'autre solution est le mode d'exploitation All Externe. Cela correspond à louer un serveur en « Housing » et à y déployer l'Application Server. Cette solution est beaucoup plus sécurisée que la précédente, car l'infrastructure autour du serveur est spécialement aménagée pour.

Dans l'absolu, un Application Server peut être presque gratuit, même s'il en existe des propriétaires dont le prix est relatif au niveau de performance. Cependant une entreprise ne va pas choisir de déployer un Application Server alors qu'elle n'en a pas besoin, car son installation et sa gestion sont beaucoup plus lourdes que ceux d'un Web Engine. Ce qui coûtera cher, ce n'est donc pas forcement l'Application Server lui-même, mais bien sa programmation.

Maintenant que ce composant est analysé, nous allons faire l'analyse du Web Engine, qui est assez proche, nous le verrons, de celle de l'application server.

2.4.3 Web Engine

a) Introduction

Les Web Engine existant sont principalement PHP, ASP, Macromedia ColdFusion et JSP. Il faut bien faire la différence entre le Web Engine qui va interpréter le langage de script, et le langage de script lui-même. PHP est à la fois un langage de script et un interpréteur, tandis qu'avec ASP, les langages de script seront JScript ou VBScript. [Wr04]

b) Etude

Nous avons vu dans les définitions les différences entre le Web Engine et l'Application Server. Ces différences portent sur des fonctionnalités en plus ou en moins, mais le travail réalisé par l'un et par l'autre est le même : effectuer le traitement de l'information. Toutes les remarques sur la sécurité et sur les modes d'exploitation de l'Application Server s'appliquent donc au Web Engine. Le choix entre le déploiement d'un Web Engine ou d'un Application Server sera fait à un niveau de design qui ne rentre pas dans le cadre de cette recherche.

2.4.4 Relational Database

a) Introduction

Pour étudier le composant « Base de Données », nous allons commencer par dresser un portrait des éléments de sécurité liés à son exploitation. Ensuite nous allons expliquer les aspects qui sont liés à chaque mode d'exploitation de la Base de Données.

b) Sécurité

Dans une architecture e-business, la Base de Données contient toutes les informations sensibles : les privilèges des utilisateurs, les transactions, les comptes clients, ... et doit par conséquent faire l'objet d'une grande précaution. [Gh99]

Pour fournir un niveau de sécurité suffisant, les principaux développeurs de Bases de Données mettent au point des techniques de chiffrement des données dans la Base qui, bien configurées, offrent un niveau de sécurité élevé. Cependant, les options par défaut permettant que la Base de Données soit fonctionnelle le plus rapidement possible ne fournissent pas un niveau suffisant de sécurité. [Gh99]

Un des éléments fondamentaux de la sécurité des Bases de Données est la configuration du contrôle d'accès. Sans cela, n'importe qui pourrait placer, modifier, ou supprimer une entrée dans la Base de Données. Plusieurs politiques d'accès peuvent être mises en place parallèlement, qu'il s'agisse par exemple de l'ajout ou de la consultation de données. La politique d'accès peut également varier en fonction de l'origine de la requête : elle peut être effectuée soit en local soit à partir d'Internet. Remarquons cependant que le fait d'effectuer une requête en local ne devrait pas constituer un assouplissement des règles d'accès. En effet, une attaque peut également provenir de l'intérieur. [Gh99]

Un dernier point à prendre en compte dans l'administration d'une Base de Données est que même si les données sont chiffrées sur le réseau, un programme doit les déchiffrer pour traiter la requête. Ces programmes peuvent utiliser des fichiers temporaires, qui peuvent être des sources de vulnérabilité. [Gh99]

c) *Bases de Données et Modes d'Exploitation*

Le lecteur pourra trouver un détail de nos recherches dans l'annexe C. Lorsqu'on travaille avec des Bases de Données, les compétences de gestion requises ne sont pas disponibles en interne. Des quatre modes d'exploitation, il n'en reste donc que deux : « Intermédiaire 1 » et « Tout Externe ».

Intermédiaire 1

Après une étude de la disponibilité des Bases de Données, les sous-modes d'exploitation disponibles sont : Achat du logiciel existant (le développement d'une Base de Données sur mesure coûte trop cher) avec le matériel acheté, et achat du logiciel existant avec matériel loué. Il faudra donc acheter ou louer le matériel qui pourra supporter ces solutions. En fonction de l'utilisation de la Base de Données, un simple ordinateur personnel pourra être suffisant, et dans d'autres cas un mainframe sera nécessaire. Dans ce sous mode d'exploitation, deux types de logiciel existent : les Bases de Données gratuites (ou libres) et les Bases de Données propriétaires. Voyons quels peuvent être les avantages et les inconvénients de ces deux alternatives.

Le principal avantage des Bases de Données gratuites est qu'elles sont disponibles immédiatement et sans frais. Cependant le coût d'achat ne doit pas rester le seul aspect. Un inconvénient est qu'il n'y a pas de service après-vente, et les interventions proposées par les développeurs du logiciel peuvent être très chères (à tire indicatif, un service d'aide via email coûte au minimum $1000 par an). D'autres difficultés potentielles pour les PME à souligner sont imputables aux caractéristiques du logiciel libre : la plupart des logiciels tournent sous Linux, ce qui représente une difficulté supplémentaire pour l'utilisateur novice en informatique. En outre, les logiciels sont en permanente évolution, et nécessitent donc des mises à jour régulières.

En ce qui concerne les Bases de Données propriétaires, le prix varie fortement en fonction de l'utilisation qu'on va en faire. Les versions personnelles (1 seul utilisateur) sont accessibles à partir d'une centaine d'euros, et les versions Multi-Utilisateurs coûtent entre 400 et 1000 euros. L'avantage d'acheter une Base de Données propriétaire est qu'il existe toujours -à part quelques exceptions- un service après vente (d'une durée limitée). Certaines Bases de Données conçues pour supporter de lourdes charges de travail existent, leurs prix pouvant dépasser les 50.000 euros.

Etant donné que la Base de Données fait partie d'une architecture e-business et qu'elle doit être disponible via Internet, l'entreprise devra se munir de l'infrastructure sécurisée particulière. Celle-ci restant bien souvent hors de prix pour une petite structure, la PME risque de ne pas être capable d'atteindre un niveau de sécurité suffisant pour protéger des données sensibles ou vitales pour l'entreprise.

Tout Externe

Avec ce mode d'exploitation, les deux possibilités sont « Achat de logiciel existant, matériel non-inclus », et « location de la solution »

Il existe de très nombreuses solutions de location sur le marché, dont les caractéristiques varient fortement. Les prix varient de 0 à 250 euros par personne par mois. Selon le fournisseur de solution, les données vont être sauvegardées tous les jours, toutes les semaines, ou jamais ; les informations échangées entre le client et la Base de Données vont être chiffrées (SSL 128 bits) ou non ; un service après-vente pourra être inclus ; la période de préavis lors de la rupture d'un contrat va varier de 0 jours à 2 mois et le nombre de requêtes faites par mois peut être limité.

Il faut remarquer que dans le cas du mode d'exploitation « Tout Externe », lors de la commande en ligne de la solution, les objectifs de performance et la politique de sécurité de la Base de Données acquise ne sont parfois pas clairement définis. Il s'agit d'y être attentif, indépendamment du prix que l'on met pour acquérir la Base de Données.

Une autre solution est l'achat du logiciel, matériel non-inclus. Cette solution est assez proche de l'Intermédiaire 1, à la seule différence que la Base de Données choisie ne sera pas installée en interne, mais sur une machine louée, en Housing (cfr. Supra). C'est une personne externe à l'entreprise qui va se charger de l'administration du serveur de la Base de Données, voire de la gestion. L'entreprise y accèdera à distance et pourra effectuer des commandes élémentaires.

Cette solution est beaucoup plus sécurisée que le mode d'exploitation Intermédiaire 1, car les serveurs loués auront un niveau de sécurité beaucoup plus spécialisé et seront mieux administrés : détecteur de fumée et d'humidité, dédoublement du système d'alimentation électrique, firewall matériel dédiés, duplication des données hors-site automatiques…

Nous pouvons conclure en disant que le mode d'exploitation qui semble le plus approprié semble être le Tout Externe.

2.4.5 Access Control

a) Introduction

Il existe des contrôles d'accès à tous les niveaux informatiques : login de l'OS, connexion au réseau, utilisation d'un logiciel... Dans ce cadre-ci, le contrôle d'accès correspond à celui de l'utilisateur de l'architecture e-business qui va vouloir accéder à une ressource. Par exemple, lorsque le client d'un site de vente en ligne va vouloir consulter l'historique de ses achats, comment s'assurer que cette personne accède aux bonnes informations ? Nous commencerons par expliquer des méthodes d'identification faibles et fortes, en insistant sur les points de sécurité de ces méthodes. Nous poserons ensuite la question de l'utilité d'un mode d'exploitation spécifique pour le contrôle d'accès, et nous expliquerons comment ce contrôle d'accès peut être réalisé avec un PKI, basé sur le protocole LDAP.

b) Sécurité

Il existe globalement deux types de méthode pour contrôler l'accès de fichiers ou de dossiers à des utilisateurs : un contrôle « faible » basé sur le hostname et l'adresse IP de l'utilisateur, le contrôle via nom d'utilisateur et mot de passe, et un contrôle « fort » utilisant des certificats. [Gh99]

Des techniques d'identification faibles

Il existe deux techniques d'identification faibles : une vérification basée sur le hostname et/ou l'adresse IP et une technique basée sur le couple « nom d'utilisateur - mot de passe ». Pour chacune des techniques d'identification il existe aussi différentes politiques de mises en œuvre.

Une première façon d'authentifier un utilisateur est donc de faire un contrôle sur le hostname et/ou l'adresse IP de l'utilisateur. Une vérification se basant simplement sur l'adresse IP de l'utilisateur est un test facile mais ne constitue pas une authentification forte, car des techniques d'IP-spoofing peuvent être mises en place pour se faire passer pour quelqu'un

d'autre. Des logiciels permettant de réaliser cette technique de piratage existent en téléchargement libre sur de nombreux sites, et sont utilisables par des personnes malveillantes n'ayant que très peu de connaissances techniques. Une amélioration est de faire ce que l'on appelle un « double-reverse look-up », qui consiste à enregistrer l'adresse IP de l'utilisateur, de prendre son hostname, et via une requête DNS faire une comparaison entre les deux ip's. Cette vérification est donc plus évoluée, mais contient la faiblesse de se baser sur les résultats d'un serveur DNS, qui peut lui-même avoir été piraté au préalable. Ce cas de figure n'est pas extraordinaire. De plus, le serveur DNS peut aussi renvoyer une IP contenue dans sa mémoire cache qui n'est plus d'actualité ; et ainsi l'utilisateur honnête se verrait refuser l'accès. [Gh99]

Les politiques de contrôles d'accès utilisant cette méthode sont les suivantes : soit toutes les connexions seront refusées, sauf celles faisant partie d'une liste, ou alors toutes les connexions seront acceptées, sauf celles faisant partie d'une liste de rejet. Ces listes ont la même structure ; elles forment un ensemble de couples « page, host ». Dans le cas de la première solution, la liste s'appellera « Access control list », et pour la seconde « Deny control list ». Il est évident que la seconde politique est plus flexible, mais propose beaucoup plus de risques. [Gh99]

Ce type de contrôle d'accès est facile à mettre en place, mais n'est pas considéré comme une vérification forte.

Une deuxième technique utilisée pour contrôler l'accès à des ressources est la vérification du couple « nom d'utilisateur - mot de passe ». La gestion de ce contrôle est faite par un administrateur qui doit garder une Base de Données avec ces couples, et dans la plupart des serveur Web cette persistance de données est constituée d'un fichier de couples chiffré, ou d'un fichier de login en clair, et d'un fichier chiffré de mots de passe correspondants. Ceci étant fait, l'administrateur doit dresser la liste des droits d'accès, pour que le serveur Web sache qui a accès à quoi. [Gh99]

Même si cette technique de contrôle d'accès semble garantir la confidentialité des ressources qu'elle protège, elle présente des risques. Un premier risque, qui n'est pas exclusif à cette technique particulière, est que les erreurs de configurations sont possibles, et la configuration parfaite est difficile à atteindre. La configuration devra être testée avant d'être déployée effectivement. Ensuite, au niveau d'une entreprise, il y aura des dizaines voir des centaines de logins. Il suffit que l'un des employés choisisse un mot de passe facile à deviner pour que

la sécurité de tout le système soit compromise. Une attaque basée sur dictionnaire sur plusieurs dizaines de logins conduira souvent à un succès, car la politique de sécurité n'a pas été appliquée correctement par les utilisateurs. Un autre risque est celui du fichier chiffré. Si des serveur Web utilisent une méthode forte pour le chiffrement du fichier, comme celle du DES, d'autres n'utilisent qu'un simple algorithme facilement déchiffrable, pour décourager les « script kiddies ». [Gh99]

Les deux politiques possibles pour un contrôle d'accès basé sur mot de passe sont le contrôle centralisé et le contrôle distribué. Le contrôle centralisé est celui où tous les mots de passe et toutes les « Access control list » sont dans un seul et même répertoire, ou un seul fichier. C'est la technique la plus facile à maintenir des deux, car les informations sont toujours au même endroit. Cependant si les ressources sont nombreuses, alors le fichier devra être mis à jour souvent ; c'est-à-dire que l'administrateur sera fort sollicité, car lui seul peut avoir accès à ce fichier, à nouveau pour des raisons de sécurité. L'autre solution, distribuée, consiste à donner à chaque répertoire ou fichier ses propres fichiers d'accès. Le grand avantage est que cette configuration est dynamique : si un fichier ou un dossier bouge, son ACL bouge avec lui. Le désavantage principal est que le contrôle global est difficile à maintenir, car il y a beaucoup de fichiers. En outre, plus il y a de fichiers, plus facilement un de ces fichier sera subtilisé par une personne malveillante. [Gh99]

Les deux systèmes de contrôle d'accès que nous venons de décrire ne présentent pas un haut degré de sécurité car toutes les informations d'identification sont envoyées en clair sur le réseau. Elles fournissent une solution rapide et relativement simple à administrer, et découragent les pirates sans intention directe de nuire, mais elles n'empêchent pas une personne déterminée à mener à bien son attaque. Il suffit que cette personne sniffe le réseau pour qu'elle puisse utiliser le nom d'utilisateur et le mot de passe de quelqu'un qui à des droits sur les ressources pour bénéficier des mêmes droits ; ou encore de faire de l'IP-spoofing. De plus, avec le contrôle de l'authentification, soit elle devra se faire pour toutes les pages, soit le serveur Web demandera au navigateur de créer un cookie de session. Si ce cookie n'est pas encodé, alors une personne intermédiaire peut sniffer le réseau et utiliser le cookie, ou encore utiliser un cookie qui se trouve sur un compte différent du même ordinateur.

Nous pouvons constater que même si les techniques expliquées fonctionnent plus ou moins bien avec la combinaison d'autres techniques, nous sommes en train de jouer au chat et à la souris. Il faut un contrôle qui soit plus fort que ces techniques. [Gh99]

Une méthode d'authentification forte : les certificats

Même si les techniques vues découragent un pirate, elles n'empêchent pas une personne malveillante déterminée. De plus, elles résistent peu aux attaques venant de l'intérieur d'un réseau : un employé peut sniffer le réseau de l'entreprise et voler logins et mots de passe. Il faut une technique forte d'identification des deux parties : aussi bien le serveur que les clients. Une telle identification peut être fournie avec le protocole SSL, et s'appuie sur le « 3-way-handshake » [Gh99]

L'authentification du serveur Web commence quand une requête est effectuée sur le port de connexions sécurisées du serveur. Celui-ci répond en renvoyant son certificat, contenant des informations telles que son identification et sa clé publique. Ce certificat est lui-même signé par un « certification authority » (CA), qui est cru à la fois par le serveur et le client. C'est au serveur de s'enregistrer chez un CA, et c'est le rôle du CA de vérifier que le serveur est bien celui qu'il prétend être. Si le client croit le CA –c'est-à-dire si le CA fait partie des « root certificates » inclus dans la plupart des navigateurs et des systèmes d'exploitation– le client génère une clé de session qui est chiffrée avec la clé publique du serveur. Cette clé de session sera utilisée pour effectuer un chiffrement symétrique, le temps de la session. [Gh99], [Ro01], [Si01]

Si le serveur désire authentifier le client, il peut maintenant le faire de deux façons : soit via login-password, ou via l'utilisation de certificats. Les problèmes concernant l'envoi du mot de passe en clair sur le réseau sont maintenant surmontés, car les informations seront chiffrées avec la clé de session. Une autre façon d'authentifier le client est d'utiliser un certificat, de la même façon que le serveur s'est authentifié au client, en utilisant les mêmes protocoles. [Gh99]

La procédure pour authentifier le client commence par la confirmation du serveur que la session a bien été établie. Il envoie au client une phrase chiffrée avec la clé de session. Si le client renvoie la phrase déchiffrée au serveur, alors le serveur saura que la session a été établie. Pour authentifier le client, le serveur va demander que ce dernier envoie son certificat. Pour

ce faire, il envoie une nouvelle phrase chiffrée avec la clé de session. Si le client possède un certificat, un hash de la phrase reçue du serveur et du certificat du client va être créé. Ce hash va être signé avec la clé privée du client, et le client va envoyer le hash signé, ainsi que son certificat au serveur, chiffrant le tout avec la clé de session. Le serveur pourra maintenant être sûr de l'identité du client. La dernière partie de l'identification sera pour le serveur d'envoyer un identifiant de session unique, qui sera utilisé tout au long de la session, jouant un rôle proche de celui du cookie. [Gh99]

Le problème principal de ce type d'identification « forte » est que très peu de clients ont effectivement un certificat signé par un CA, car ceux-ci coûtent très cher. Il est néanmoins possible pour le serveur de créer lui-même ce certificat, qu'il donnera au client. Le problème reviendra alors au client de pouvoir gérer tous les certificats qu'il a reçu des serveurs Web, et de les garder dans un lieu sûr. [Gh99]

Pratiquement, ces techniques sont implémentées avec les protocoles SSL (et TSL) et SET. SSL est un protocole développé par Netscape en 1994 pour fournir un certain niveau de sécurité sur Internet. Il supporte l'authentification du serveur et assure la confidentialité et l'intégrité du canal de transmission. Il opère au niveau de la couche de transport, entre TCP et HTTP, et est donc indépendant des applications. SSL chiffre complètement le canal de communication grâce à un chiffrement à clés asymétriques, mais ne supporte ni les signatures électroniques au niveau du message, ni la non-répudiation des messages. SSL v3 a été standardisé par l'IETF sous le nom de TLS (Transport Layer Security). SSL et TLS sont intégrés dans la plupart des browsers Web. Les deux ne sont pas interopérables entre eux mais un browser supportant SSL est capable de traiter les messages envoyés avec TLS. C'est un protocole général de sécurisation des communications via le réseau quoiqu'il ait été conçu au départ pour permettre la sécurisation des transactions par carte de crédit sur le Web. Les informations importantes à chiffrer sont, par exemple, les détails bancaires et le numéro de carte de crédit. Ses avantages sont qu'il propose la confidentialité et l'intégrité des données chiffrées. Il est simple, performant, populaire, et il est transparent au niveau des applications. Il présente aussi certains inconvénients, comme par exemple le fait qu'il n'y a pas de non-répudiation du message (dû au fait qu'on n'tilise pas de certificats). [Ha03]

SET est le produit de l'association des deux plus gros organismes mondiaux qui délivrent des cartes de crédit, c'est-à-dire Visa et MasterCard. D'autres entreprises ont également collaboré

au projet telles que Netscape Coporation, Microsoft, IBM, ... Le projet a débuté en 1996 et depuis, de nombreuses révisions y ont été apportées. C'est la compagnie indépendante SETCo, formée par Visa et MasterCard en 1997, qui gère ces révisions du standard. SET est un protocole qui ne s'occupe que de la partie paiement des transactions. Pour garantir la sécurité, de nombreuses techniques et algorithmes de cryptographie sont utilisées (telles que MD5, SHA, Dual signatures, RSA). Sa particularité est que le marchand ne puisse nullement avoir accès aux données bancaires du client et de même, la banque du marchand ne peut voir les détails de la transaction commerciale qui se déroule. Pour permettre l'interopérabilité, tous les messages sont définis dans un format indépendant de la machine ou de l'OS.

SET repose sur SSL, STT (Secure Transaction Technology de Microsoft) et sur S-HTTP. Dans ce système, toutes les parties doivent détenir un certificat et la paire de clés correspondante. Il doit donc exister une hiérarchie d'autorités de certification dont la racine est SETCo (depuis sa création). Trois composants principaux sont nécessaires pour permettre l'utilisation du protocole SET : un logiciel portefeuille chez le client, le serveur doit avoir le support SET installé, et l'interface de paiement doit pouvoir traiter les transactions SET et pouvoir interagir avec les réseaux financiers. [Ha03]

Ces principales forces sont que tous les messages entre les différentes parties préservent des contraintes de sécurité fortes : confidentialité, authentification, intégrité et non-répudiation des messages, et que les différentes parties sont parfaitement authentifiées. [Ha03]

Une des difficultés de SET est qu'il est décrit complètement en 3 volumes fastidieux. Cela demande donc beaucoup d'effort aux développeurs pour produire des applications répondant à ses normes. De plus, le besoin d'une hiérarchie de certification pouvant supporter le système rend le processus assez complexe. Aussi les associations de cartes de crédit qui veulent pouvoir participer au système doivent d'abord mettre en œuvre l'infrastructure nécessaire mais également passer par une procédure stricte de certification avec le niveau supérieur dans la hiérarchie. Enfin SET est un logiciel propriétaire, et nécessite donc un investissement non négligeable. [Ha03], [An01]

Le protocole SET qui semble parfait pour les transactions commerciales (confidentialité non seulement par rapport à un écoute du réseau, mais aussi par rapport à sa banque, intégrité, authentification des deux parties, et non-répudiation) n'a pourtant jamais décollé, tellement sa

mise en place est fastidieuse et coûteuse. De plus il se base sur un chiffrement à clé asymétrique des deux parties, alors que les particuliers n'ont en général pas cette paire de clé à disposition. [Ha03]

c) Utilité

Il faut envisager les avantages qu'il y aurait à pouvoir dissocier le contrôle d'accès du reste de l'architecture. En effet, ce qui est intéressant dans notre optique d'analyse du déploiement est de savoir si un composant tiers peut gérer ce contrôle d'accès à distance, et d'éviter ainsi à l'entreprise la complexité de la gestion de la sécurité et des frais de déploiement de ce contrôle. Si une entreprise désire pour des raisons de confidentialité garder sa Base de Données en interne, elle peut aussi vouloir ne pas se soucier de la gestion du contrôle d'accès.

d) Problème

Dans un environnement dynamique, le problème revient donc à savoir comment le contrôle d'accès va savoir à quelles ressources un client a accès. Si le contrôle d'accès porte sur le champ d'une table, alors il sera difficile pour le fournisseur du contrôle d'accès d'effectuer un contrôle s'il n'est pas directement relié au système de persistance de données de l'entreprise.

e) Solution

Les deux solutions envisageables peuvent être réalisées par la mise en place d'un PKI. Celui-ci permet aux clients de l'architecture de se connecter, de s'authentifier sur un serveur via leur navigateur (ou un client très léger) et d'accéder à un certain nombre de ressources. Ces ressources peuvent être du code exécutable, donc ce type de contrôle d'accès permet à l'entreprise de complètement déléguer son contrôle d'accès à un tiers.

Introduction au PKI

Un « PKI », acronyme de « Public Key Infrastructure », est défini par l'ensemble de techniques, organisations, procédures et pratiques qui définissent l'implémentation et l'exploitation de certificat numériques basés sur la cryptographie à clés publiques. [Be03]

L'adoption de solutions de sécurité basées sur la cryptographie à clés publiques nécessite la mise en place d'une infrastructure de gestion des clés et des certificats. Cette infrastructure est composée des éléments logiciels, matériels et humains, ainsi que des procédures pour créer,

gérer, distribuer les clés privées et les certificats utilisés par les applications de sécurité des clients finaux.

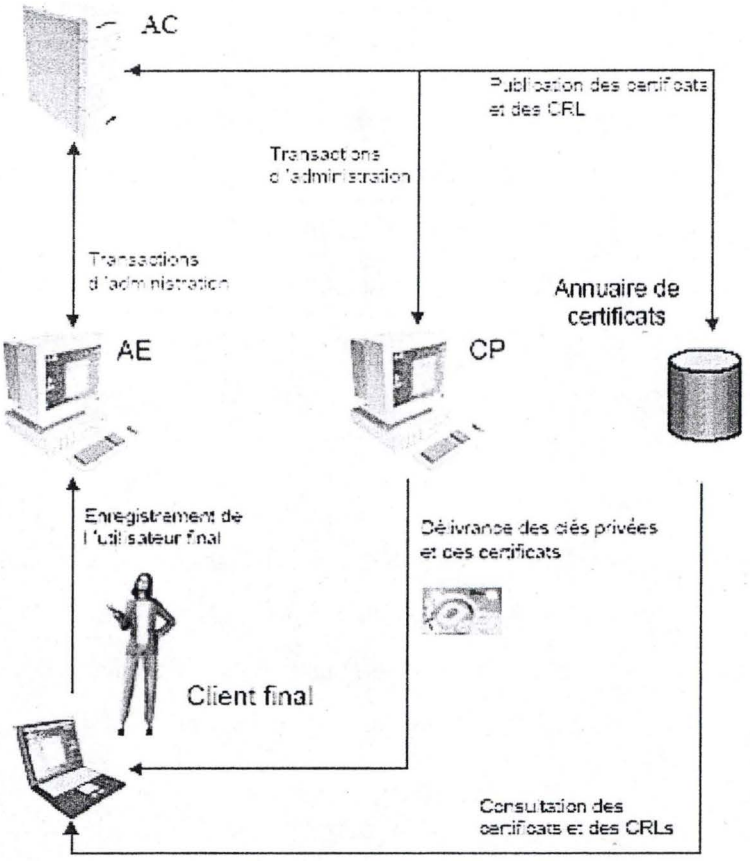

Fig. 3.4– Eléments d'une PKI

Comme le montre le figure [Fig. 3.4], le déploiement d'une PKI nécessite la mise en place de quatre composants :

- Une autorité d'enregistrement (AE) assurant le lien entre l'identité du client final et les éléments secrets qui lui seront affectés (clé privée et certificat).
- Une autorité de certification (AC) assurant la création et la révocation des certificats demandés par l'AE.
- Un centre de personnalisation ou de distribution (CP) permettant de délivrer les clés privées et les certificats aux clients finaux sous forme d'un fichier informatique ou d'un support physique (carte à puce ou clé USB).
- Un annuaire dans lequel les certificats publics seront publiés afin d'être accessibles aux clients finaux désirant correspondre.

[Mi00]

Les fonctions principales offertes par la PKI sont les suivantes :

- L'enregistrement : cette opération consiste à enregistrer dans la base de la PKI les informations nominatives sur le client final qui désire disposer de clés privées et de certificats. Un formulaire standard doit être renseigné pour chaque personne. Ce formulaire invite à saisir un nom, un prénom, la société, le département, l'adresse, un numéro de téléphone et de télécopie et une adresse email.
- La génération des clés : L'opération de production des clés consiste à générer les paires de clés privées et publiques qui seront utilisées par les fonctions de certification et de personnalisation.
- La certification : sur la base des éléments du client final enregistré, l'AC de la PKI élabore les certificats.
- La publication : les certificats générés peuvent êtres publiés dans un annuaire LDAP.
- La révocation : si un changement intervient dans le profil d'un client ou si les clés privées qui lui ont été affectées sont compromises, ses certificats doivent êtres révoqués. La révocation d'un certificat consiste à l'inscrire dans une liste de révocation (CRL) accessible elle-même dans un annuaire. La fréquence de publication de la CRL est paramétrable pour tenir compte du niveau de sécurité désiré. [Mi00]

L'utilisation de clefs asymétriques entraîne la nécessité de la publication en toute confiance de la clef publique. Cette publication doit assurer la validité d'une clé et l'appartenance de cette clé à la bonne personne. La publication des certificats (des clefs publiques) est faite en utilisant les structures d'annuaires de type LDAP (Lightweight Directory Access Protocol), que nous allons expliquer brièvement.

LDAP

Le LDAP est un protocole définissant un standard pour accéder aux informations contenues dans un répertoire. C'est un protocole ouvert, indépendant d'un vendeur, d'une configuration matériel, logiciel ou de réseaux particulier. Il est léger en comparaison au protocole DAP, qui est une partie de l'ancien protocole d'accès aux répertoires pour les réseaux : X.500. Il est donc plus simple, plus rapide, moins sécurisé, et plus léger que ce dernier. Il permet d'utiliser un service de répertoires avec des technologies comme ATM ou FDDI. [Ho03], [Sh03]

Un répertoire est un genre de Base de Données spécialisé. Il est conçu pour supporter un grand nombre de lectures, et peu d'écritures. Il offre une vue statique des données et ne supporte pas d'opérations transactionnelles. Les informations contenues dans un répertoire peuvent être : une organisation, des gens, des fichiers, des périphériques…

Le protocole X.500 est un protocole client/serveur permettant d'accéder à des répertoires. Les trois composants principaux sont le DUA, le DSA et le DAP. Le DUA, Directory User Agent, est le composant côté client. Il fournit au client les fonctionnalités de recherche et de navigation dans les Bases de Données de répertoires. Le côté serveur est le Directory System Agent (DSA) : c'est la Base de Données dans laquelle les répertoires sont stockés. Le DAP est le protocole de communication entre le DUA et le DSA. Il permet aux clients d'accéder aux répertoires sans connaître l'emplacement géographique exact de ceux-ci. X.500 à été jugé trop complexe pour la plupart des utilisations que l'on voulait en faire, et c'est pour contourner cette lacune que le protocole LDAP à été conçu. [Ho03], [Sh03]

Son fonctionnement est le suivant : un client se connecte au serveur, effectue des opérations, et puis se déconnecte. Ces opérations sont : se « lier » au serveur (s'y authentifier), chercher une entrée, comparer des entrées, ajouter une entrée, modifier une entrée et retirer une entrée.

Techniquement, chaque entrée dans un répertoire est unique et hiérarchique. Un peu comme pour la construction d'une url, le nom d'un répertoire est fonction du nom du répertoire au-dessus de lui. Le protocole LDAP offre des services de sécurité tels l'authentification, la confidentialité et l'intégrité. [Ho03], [Sh03]

Ses utilisations sont multiples : la plupart des clients mails, comme Outlook Eudora, et Netscape Communicator utilisent une Base de Données LDAP pour trouver des adresses email. Etant donné que les entrées dans un répertoire peuvent être à peu près n'importe quoi, y compris du code exécutable ou du code SQL, les utilisations de LDAP sont très variées. [Ho03], [Sh03]

Même s'ils peuvent sembler pareils, les serveurs LDAP et les RDBMS sont conçus pour fournir un type d'information différent. LDAP est globalement un mécanisme d'accès. Un RDBMS pourrait donc émuler un LDAP. Cependant un serveur LDAP est plus rapide qu'un RDBMS pour fournir des informations sous forme de « pages blanches » ou de « pages

jaunes », car ils sont conçus pour faire beaucoup plus d'accès en lecture qu'en écriture. [Ho03], [Sh03]

Cependant, cette solution pourrait bien ne pas être la meilleure, car bien que le LDAP soit une version « light » du protocole X.500, il évolue vers un service de répertoires complet. Il utilise un Naming Service complexe, et des couches de sécurité sont ajoutées. Des fonctionnalités existantes dans X.500 sont ajoutées elles aussi, si bien que certains spécialistes estiment que lorsque les certaines fonctionnalités manquantes au LDAP seront ajoutées (contrôle de sécurité, réplication de Bases de Données hors-site, utilisation de caractères autres que le ASCII standard), il deviendra aussi complexe que X.500. [Ho03], [Sh03]

f) Faiblesse d'un PKI

Malgré tout les avantages que nous venons de présenter, l'utilisation d'un PKI au sein de petites ou même des grandes structures est compromise, dû à un certain nombre de raisons, la principale restant financière : pour pouvoir obtenir des paires de certificats signés, il faut mettre le prix, car le AC doit lui-même payer pour être présent dans les « root certificates » de Windows et d' Internet Explorer. Mais il y a d'autres problèmes, liés à la structure intrinsèque des certificats : les clés ne sont pas des gens. Tout ce qu'un certificat prouve, c'est qu'une personne qui signe à l'aide d'une signature numérique à accès à une clé privée particulière qui correspond à une clé publique particulière qui appartient à un CA particulier. Rien de plus ! Toute la sécurité du système repose sur l'utilisateur ; si la clé privée est volée, ou qu'un virus modifie le code du navigateur pour qu'il génère toujours la même clé, toute la sécurité du système est mise à mal. [Ga02]

De plus, y a un manque de respect de la vie privée avec la gestion des PKI actuels. Si une personne à un seul et unique identifiant, il est très facile de croiser des Bases de Données, et d'ainsi établir un profil. Par exemple, pour une personne particulière, on pourrait croiser les Bases de Données de ses comptes bancaires, avec son salaire, les kilomètres parcourus en voiture, les paiements par carte de crédit, les livres qu'il lit, ses appels téléphoniques, ... [Ga02]

2.4.6 Encryption

a) Introduction

Nous terminons cette deuxième partie par l'analyse du composant « Encryption ». Nous verrons quels modes d'exploitation sont possibles pour son utilisation.

b) Utilité

Ce composant est utilisé pour assurer entre autre une communication confidentielle entre le serveur Web et le client, mais il est également utile pour des fonctions telles que la gestion à distance. Pour effectuer cette gestion à distance, le protocole SSH c'est imposé comme le standard actuel. Différentes implémentations du protocole existent, certaines en Open Source, et d'autres payantes. C'est un protocole de communication sécurisée permettant l'accès distant à des machines Unix (en remplacement de commandes telles que rlogin, rsh et rcp qui ne sont pas sécurisées). Il est utilisé énormément par des administrateurs de réseaux Web ou autres. OpenSSH permet de pallier les faiblesses de sécurité des accès distants aux systèmes Unix (ex. : telnet, X11) en fournissant les services de sécurité. Son principal inconvénient, pour les petites structures, est qu'il ne fonctionne pas sous windows. De plus la gestion à distance n'est, par définition, pas destinée à la PME elle-même. [Gh99], [Ha03], [Va03]

c) Encryption et Modes d'exploitation

Quel que soit le niveau de sécurité requis ou les fonctionnalités requises, le composant encryption devra se situer au même endroit que le serveur Web et que le contrôle d'accès, et l'administration ne pourra pas être faite par la PME. Il faudra donc outsourcer les compétences de gestion de ce composant, car même si l'une ou l'autre opération peuvent être effectuées par la PME, la configuration de ce composant requiert un niveau d'expertise élevé pour atteindre un niveau de sécurité irréprochable.

Nous venons de caractériser chaque composant de l'architecture les plus indépendamment possible des autres. Nous avons vu que les quatre modes d'exploitation que nous avons identifiés dans notre typologie ne sont pas envisageables pour tous les composants. Il ressort qu'il n'y a que deux modes d'exploitation sécurisés possibles pour presque tous les composants : le Tout Externe et l'Intermédiaire1. Partant de ce constat, nous allons à présent

procéder à l'analyse de l'architecture prise dans son ensemble en fonction de ces deux modes d'exploitation.

Chapitre 3 : Architectures e-business : étude intégrée de la sécurité en fonction du mode d'exploitation.

3.1 Introduction

Sur base de ce que nous venons d'analyser, nous allons tenter de conclure en proposant le mode d'exploitation qui semble convenir le mieux aux PME.

3.2 Evaluation

Nous avons montré que les modes d'exploitation possibles pour utiliser de façon sécurisée une architecture e-business pour une PME sont le Tout Externe et l'Intermédiaire 1. La sécurité étant définie en terme de confidentialité, d'intégrité, et de disponibilité, il nous semble pertinent de suivre cette définition pour faire l'analyse des deux modes d'exploitation.

3.2.1 Confidentialité

La confidentialité concerne deux aspects : la confidentialité des informations de l'entreprise enregistrées dans la Base de Données, et la confidentialité des opérations effectuées avec l'extérieur, dans le cas d'opération B2C ou B2B. Par conséquent, les deux composants directement concernés par les aspects de la confidentialité sont la Base de Données, qui contient toutes les informations de l'entreprise, et le serveur Web, qui est la vitrine de l'entreprise vis-à-vis de l'extérieur.

Premièrement, pour la confidentialité des informations qui circuleront sur Internet, nous pouvons considérer que le niveau de sécurité est équivalent dans les deux modes d'exploitation. En effet, dans les deux cas, ce sont des professionnels qui se chargeront de l'installation, de la configuration, et de la maintenance des logiciels de l'architecture. La localisation n'aura pas d'influence sur la configuration.

Voyons ce qu'il en est concernant la Base de Données. Si l'architecture est déployée en interne, il est très important que chaque personne ayant un accès physique à la salle de

machines puisse être identifiée et tracée, dans les respects de la vie privée bien entendu. Si elle est déployée en externe, des personnes étrangères à l'entreprise y ont potentiellement accès. Il faut alors prendre des précautions au niveau contractuel quant aux clauses de confidentialité, et il faut également se munir des outils juridiques nécessaires. Il va de soi qu'une entreprise ne souhaite pas qu'un concurrent puisse avoir accès à ses fichiers, et que tout doit être mis en œuvre pour l'éviter.

3.2.2 Intégrité

Le problème de l'intégrité se retrouve principalement dans les protocoles de chiffrement, qui sont indépendants de la localisation propre des composants. Le mode l'exploitation de l'architecture n'aura pas d'influence sur l'intégrité des données.

3.2.3 Disponibilité

La disponibilité se divise en deux parties : la disponibilité logique, et la disponibilité physique. La première peut être affectée par une attaque logique, de type Denial of Service (DoS), la seconde par une attaque physique ou un désastre.

Dans la conclusion de notre étude du Housing, nous avons vu que pour une petite structure, posséder une salle informatique offrant une bonne disponibilité (résistante à tout type de désastre, et pouvant répondre à un nombre potentiellement grand de requêtes simultanées) est quasiment impossible, principalement au niveau du coût.

Pour un même niveau de sécurité, la différence de coût entre les deux types de déploiement est trop importante. Si l'on prend en considération que la sécurité doit être rentable, le niveau de sécurité du mode d'exploitation Intermédiaire 1 est alors trop faible.

Pour la plupart des PME, c'est probablement à ce niveau de sécurité que la différence de mode d'exploitation aura le plus d'impact sur le niveau de sécurité général de l'architecture : un manque de moyens ne permet pas de déployer une architecture sécurisée.

3.2.4 Conclusion

Parmi les quatre modes d'exploitation identifiés, nous avons vu que seuls deux sont envisageables : il s'agit de l'intermédiaire 1 et du Tout Externe.

Nous avons vu qu'au niveau de la confidentialité, il était préférable d'avoir l'architecture en interne. Si cette option n'est pas envisageable, nous avons vu que l'entreprise peut se munir des outils juridiques et contractuels nécessaires et de cette manière, elle peut maintenir un niveau de confidentialité suffisant en déployant son architecture en externe. [Go01] Le problème de la disponibilité ne peut quant à lui être soulevé de la même manière. Investir dans une infrastructure coûteuse est la seule manière d'assurer la disponibilité, mais un tel investissement reste difficile pour la plupart des PME…

Face à ce constat, nous pouvons conclure qu'en ce qui concerne la sécurité, le mode d'exploitation le plus adéquat aux architectures e-business que nous avons définies pour la PME est le « Tout Externe ».

Cette conclusion doit cependant être nuancée. Si nous pensons qu'elle s'applique dans de nombreux cas de figures, il n'en demeure pas moins qu'il existe des entreprises de grande taille qui n'ont pas de compétences en informatique (et qui donc entrent dans notre définition des PME), et qui, pour des raisons de confidentialité, ne veulent externaliser leur système de persistance de données. Ainsi, nous pourrions envisager par exemple le cas d'un hôpital, qui pourrait justement avoir les moyens d'acquérir cette infrastructure sécurisée en interne.

Conclusion

Arrivé au terme de ce travail, nous allons retracer le parcours qui, d'une mission qui nous a été donnée dans le cadre de notre stage, a abouti à la proposition d'une typologie des modes d'exploitation et à des conclusions générales permettant de dire quel est, parmi les quatre modes d'exploitation identifiés, le plus adéquat pour les PME en se centrant sur les contraintes de sécurité.

L'objet de ce travail était de faire une étude de la sécurité des architectures e-business pour les PME en fonction de leur mode d'exploitation. Dans la première partie, nous avons commencé par définir les concepts principaux sur lesquels repose notre mémoire. C'est ainsi que nous avons explicité l'acceptation particulière que nous donnions aux termes PME, e-business, architecture e-business, modes d'exploitation, et sécurité, ces deux dernières notions ayant fait l'objet d'un développement plus approfondi. Nous avons également présenté le cadre de recherche dans lequel notre mémoire s'inscrit, et avons expliqué, dans notre deuxième partie portant sur la méthodologie, notre rôle au sein du projet Acces-PME et notre manière de procéder. Dans notre troisième partie, que nous avons intitulé « partie recherche », nous avons proposé une typologie des modes d'exploitation en prenant en compte deux variables liées à la localisation : la localisation de la solution informatique d'une part, et la localisation des compétences d'autre part. A partir des travaux de V. Rosener qui définit deux types d'architectures e-business en en identifiant les composants, nous avons, pour chacun d'entre eux donné tout d'abord une définition. Ensuite, nous avons abordé les aspects de sécurité relatifs à chacun de ces composants d'abord spécifiquement puis en les mettant en rapport avec chaque mode d'exploitation possible.

Nous avons constaté que seuls deux modes d'exploitation sont envisageables pour une utilisation sécurisée d'une architecture e-business pour les PME : le mode Tout Externe et l'intermédiaire 1. Afin de pouvoir comparer ces deux modes d'exploitation en termes de sécurité, nous avons repris les trois critères définitoires du terme « sécurité », et les avons analysé en regard des deux modes d'exploitation. Il ressort que le mode d'exploitation Tout Externe est, toujours en termes de sécurité et pour les PME, le plus approprié pour l'exploitation sécurisée de la plupart des architectures e-business.

Ce travail comporte des limites.

Vu l'étendue de la mission qui nous fut confiée, nous nous rendons compte que bon nombre de concepts auraient pu faire l'objet de plus amples développements, ou auraient pu faire l'objet d'un développement tout court. Ainsi, par exemple, nous aurions souhaité pouvoir aborder davantage les questions de sécurité liées au navigateur client. Lors d'études ultérieures, il nous semblerait intéressant d'intégrer l'étude de ce composant.

En outre, les grilles de questions que nous avons élaborées et qui nous ont permis de caractériser les composants en fonction de leur mode d'exploitation le furent sur base de critères subjectifs, qui n'ont pas fait l'objet d'une étude de validité et de fiabilité scientifique. Par conséquent, les observations que nous en avons tirées sont elles aussi empruntes de subjectivité. Il nous semblerait dès lors intéressant, lors d'une étude ultérieure, de faire une analyse approfondie et systématique des offres des différents composants afin d'en détecter les avantages et les lacunes. Une telle étude permettrait éventuellement de confirmer ce que nous avons constaté dans notre pratique quotidienne de stagiaire.

Bibliographie

Livres

[Al03] D. Alur, J. Crupi, "Introduction à J2EE", J2EE et les Design Patterns, CampusPress , Paris, pages 11-21, févr-03

[An01] R. Anderson, Security Engineering, John Wiley & Sons, Inc., New York, 2001

[Gh99]A. K. Ghosh, E-Commerce Security. Weak Links, Best Defenses, Wiley Computer Publishing, New York, NY, 1999

[Ga02]S. Garfinkel, Web Security, Privacy, and Commerce, Second Edition, O'Reilly & Associates, Inc, Sebastopol, California, 2002

Thèses

[Go01] J.-B. Gosuin, L'application Sercie Provider : une solution informatique pour les PME ?, PhD thesis, Facultés Universitaires Notre Dame de la Paix, Namur, 2002

[Ha03] R. Hallez, OpenSST: Format de message et protocole de transfert sécurisé de données, PhD thesis, Facultés Universitaires Notre Dame de la Paix, Namur, 2003

En ligne

[Be03] M. Benjada, Les PKI, http://www.securiteinfo.com/crypto/pki.shtml, Date d'accès: déc-03

[Ce04] Center for Software Engineering, Beyond 9126 - ITSEC, http://www.cse.dcu.ie/essiscope/sm2/beyond/itsec.html, Date d'accès: Date d'accès: avr-04

[Co04] Corsec, Common Criteria Summary, http://www.corsec.com/ccc_summary.php, Date d'accès: avr-04

[Dr02] P. Drayton, What is .NET?, http://www.razorsoft.net/weblog/stories/2002/02/10/whatIsnet.html, dernière mise à jour: 7-juil-02, Date d'accès: janv-04

[Ho03] J. Hodges, Introduction to Directories and the Lightweight Directory Access Protocol, http://www.stanford.edu/~hodges/talks/mactivity.ldap.97/index2.html, Date d'accès: decembre 2003

[Li04] A. Lioy, Security Standards, www.setcce.org/natows/slides/SecStd.pdf, Date d'accès: avr-04

[Mi00] M. Milan, Infrastructures à clés publique, http://www.trustycom.fr/docs/Aristote_pki1.ppt, dernière mise à jour: 20-janv-00, Date d'accès: déc-03

[Pi04] J.-F. Pillou, Les systèmes RAID, http://www.commentcamarche.net/protect/raid.php3, Date d'accès: mai-04

[Ro01] D. Robbins, OpenSSH key management, Part 1, http://www-106.ibm.com/developerworks/library/l-keyc.html, dernière mise à jour: 1-juil-01, Date d'accès: nov-03

[Ry04] Rycombe, ITSEC summary, http://www.rycombe.com/itsec.htm, dernière mise à jour: 2004, Date d'accès: Date d'accès: avr-04

[Se01] R. Sessions, Java 2 Enterprise Edition (J2EE) versus The .NET Platform. Two Visions for eBusiness, http://www.objectwatch.com/FinalJ2EEandDotNet.doc, dernière mise à jour: march 28, 2001, Date d'accès: janv-04

[Sh03] B. Shuh, Directories and X.500: An Introduction., http://www.collectionscanada.ca/9/1/p1-244-e.html, Date d'accès: decembre 2003

[Si01] R. Sigle, Building a Secure RedHat Apache Server, HOWTO, http://www.tldp.org/HOWTO/SSL-RedHat-HOWTO.html, dernière mise à jour: 2 juin 2001

[Un01] unknown, What is a TP monitor?, http://www.webopedia.com/TERM/T/TP_monitor.html, dernière mise à jour: 6-déc-01, Date d'accès: avr-04

[Un04] Unknown, Message-Oriented Middleware, http://www.sims.berkeley.edu/courses/is206/f97/GroupB/mom/what_is_mom.html, dernière mise à jour: 2004, Date d'accès: janv-04

[Va03] S. Vance, Gain secure remote login with SSH, http://www.palmpowerenterprise.com/issues/issue200206/sshclient001.html, Date d'accès: nov-03

[VR01] C. Vawter, Ed Roman, J2EE vs. Microsoft .NET, http://www.theserverside.com/ressources/article.jsp?l=J2EE-vs-DOTNET, dernière mise à jour: june 2001, Date d'accès: janv-04

[Wr04] J. C. Wright, Net Technologies and What They Mean To You, http://www.scene360.com/ARTdirect_webdesign_tech_01.html, Date d'accès: janv-04

Autres

[HW99] R. Henrion, Claude Wehenkel, Convention Relative au Projet Acces-Pme, Luxembourg, 1-janv-99,

[Ke03] B. Kechicheb, Exigences de Sécurité, Acces-Pme, Luxembourg, 2003

[Ro04] V. Rosener, Architectures e-business sécurisées, Acces-Pme, Luxembourg, 2004

1. Annexe A - Housing - Etude de l'existant

Critères

Vendeur

Nom de l'offre

Caractéristiques techniques

- Type de serveur
- Taille du disque dur (GB)
- Transfert par mois (GB)
- Bande passante
  - Garantie (oui / non)
  - Taille (Mb/s)
- Extensibilité possible (disque dur, volume/mois…)

Fiabilité du fournisseur de la solution

- Type de contrat
- Durée du préavis lors de la rupture de contrat
- Année de la commercialisation de l'offre
- Signalisation de la localisation du serveur

Sécurité

- Clarté de la politique de sécurité
- Duplication des données
- Duplication du hardware
- Backups
- Uptime garanti

Prix (euros)

- Initialisation
- Par mois

Service après-vente

- Inclus dans le prix d'achat
- Coût d'une intervention

Etude de cas

Vendeur : luxhosting.lu (http://www.luxhosting.lu/serveurs.php)

Nom de l'offre : RaQ3 – RaQ4i – RaQ4r – RaQ550

Caractéristiques techniques

Type de serveur : Sun Cobalt
Taille du disque dur : 10 – 20 – 30 – 80
Transfert par mois (GB) : 10 – 20 – 20 – 20
Bande passante
Garantie : oui
Taille : inconnue
Extensibilité possible : partielle (ram, transferts)

Fiabilité du fournisseur de la solution

Type de contrat : inconnu
Durée du préavis lors de la rupture de contrat : 30 jours
Année de la commercialisation de l'offre : 1999
Signalisation de la localisation du serveurs : oui

Sécurité

Clarté de la politique de sécurité : pas claire… La façon dont le hardware est protégé est inconnu.
Duplication des données : non – non – oui – option
Duplication du hardware : carte réseau.
Backups : en option
Uptime garanti : 99.9%

Prix (euros)

Initialisation : 99 – 199 – 249 – 459
Par mois : 49 – 199 – 249 – 459

Service après-vente

Inclus dans le prix d'achat : oui
Coût d'une intervention : 0

Vendeur : cdr-house.com (http://www.cdr-house.com/hosting/hosting.asp)

Nom de l'offre : Standard Server – Advanced Server

Caractéristiques techniques

Type de serveur : Inconnu
Taille du disque dur : 4 (SCSI) – 15 (SCSI)
Transfert par mois (GB) : 10 - 20
Bande passante
Garantie (oui / non) : non
Taille (Mb/s) : inconnue
Extensibilité possible (disque dur, volume/mois…) : hardware et software sur demande

Fiabilité du fournisseur de la solution

Type de contrat : signature électronique du SLA
Durée du préavis lors de la rupture de contrat : 30 jours
Année de la commercialisation de l'offre : 2001
Signalisation de la localisation du serveurs : non

Sécurité

Clarté de la politique de sécurité : sécurité physique inconnue
Duplication des données : oui
Duplication du hardware : disques durs
Backups : oui si pas de raid
Uptime garanti : 99.9%

Prix (euros)

Initialisation : 900 - 2600
Par mois : 500 - 1100

Service après-vente

Inclus dans le prix d'achat : 8 heures / mois
Coût d'une intervention : inconnu, support par mail gratuit

Vendeur : root eSolution (http://www.root.lu/?site=housing)

Nom de l'offre : basic – rooted (2 intermédiaires)

Caractéristiques techniques

Type de serveur : inconnue
Taille du disque dur (GB) : inconnu
Transfert par mois (GB) : 4 – 30
Bande passante
Garantie (oui / non) : non
Taille (Mb/s) : inconnu
Extensibilité possible (disque dur, volume/mois…) : inconnu

Fiabilité du fournisseur de la solution

Type de contrat : inconnu
Durée du préavis lors de la rupture de contrat : 0 jours
Année de la commercialisation de l'offre : 2003
Signalisation de la localisation du serveurs : oui

Sécurité

Clarté de la politique de sécurité : très claire
Duplication des données : inconnu
Duplication du hardware : inconnu
Backups : inconnu
Uptime garanti : 99.99%

Prix (euros)

Initialisation : 50 – 50
Par mois : 80 – 200

Service après-vente

Inclus dans le prix d'achat : par mail
Coût d'une intervention : mail : 0 – premium support : inconnu

Vendeur : LuxAdmin (http://www.luxadmin.org/housing.php)

Nom de l'offre : Privat – Hosting

Caractéristiques techniques

Type de serveur : inconnu
Taille du disque dur (GB) : inconnu
Transfert par mois (GB) : 4 - 16
Bande passante
Garantie (oui / non) : non
Taille (Mb/s) : inconnue
Extensibilité possible (disque dur, volume/mois…) : oui

Fiabilité du fournisseur de la solution

Type de contrat : inconnu
Durée du préavis lors de la rupture de contrat : 0 jours
Année de la commercialisation de l'offre : 1999
Signalisation de la localisation du serveurs : oui

Sécurité

Clarté de la politique de sécurité : Bonne
Duplication des données : inconnu
Duplication du hardware : inconnu
Backups : réguliers
Uptime garanti : non

Prix (euros)

Initialisation : 50 – 50
Par mois : 35 – 110

Service après-vente

Inclus dans le prix d'achat : mail
Coût d'une intervention : 80 euros

2. Annexe B - Web Server - Etude de l'existant

Critères :

Fournisseur
Site :
Nom du service :

Serveur dédié (o/n)

Sécurité
- Chiffrement des données lors des échanges (o/n)
- Garantie de la bande passante
- Uptime garanti
- Duplication des données (o/n/fréquence)

Fiabilité du fournisseur de la solution
- Durée du préavis lors de la rupture du contrat
- Année de la commercialisation de la solution
- Signalisation de la localisation du serveur

Coût
- Coût initial
- Coût par mois

Volume
- De données sur le serveur
- De transfert par mois

Caractéristiques du service après-vente :
- Inclus dans le prix d'achat (oui / non / durée)
- Coût d'une intervention

1. Fournisseur : Tiscali

Site : http://telecom.tiscali.lu/product/hosting/
Nom du service : serveur partagé / serveur dédié
Serveur dédié : non / oui

Sécurité

- Chiffrement des données lors des échanges : non / oui
- Garantie de la bande passante : inconnu
- Uptime garanti : inconnu
- Duplication des données : non / oui

Fiabilité du fournisseur de la solution

- Durée du préavis lors de la rupture du contrat : inconnue
- Année de la commercialisation de la solution : 1997
- Signalisation de la localisation du serveur : non

Coût

- Coût initial : contacter le fournisseur
- Coût par mois : contacter le fournisseur

Volume

- De données sur le serveur : 25 MB / non-défini
- De transfert par mois : non-défini

Caractéristiques du service après-vente :

- Inclus dans le prix d'achat : inconnu
- Coût d'une intervention : inconnu

2. Fournisseur : Generity

Site : www.generity.net
Nom du service : Basic / Ultra

Serveur dédié : inconnu

Sécurité

- Chiffrement des données lors des échanges : inconnu
- Garantie de la bande passante : inconnue
- Uptime garanti : inconnu
- Duplication des données : inconnu

Fiabilité du fournisseur de la solution

- Durée du préavis lors de la rupture du contrat : inconnu
- Année de la commercialisation de la solution : 2003
- Signalisation de la localisation du serveur : non

Coût

- Coût initial : 0
- Coût par mois : 2 euros / 10 euros

Volume

- De données sur le serveur : 60 MB / 300 MB
- De transfert par mois : illimité

Caractéristiques du service après-vente :

- Inclus dans le prix d'achat : mail et forum
- Coût d'une intervention : inconnue

3. Fournisseur : Web Technologies s.a.

Site : www.web.lu
Nom du service : Basic / Business (2 solutions intermédiaires existent)

Serveur dédié : non

Sécurité

- Chiffrement des données lors des échanges : non
- Garantie de la bande passante : non
- Uptime garanti : non
- Duplication des données : non / quotidien

Fiabilité du fournisseur de la solution

- Durée du préavis lors de la rupture du contrat : inconnu
- Année de la commercialisation de la solution : 2000
- Signalisation de la localisation du serveur : non

Coût

- Coût initial : 0
- Coût par mois : 35 euros / 80 euros

Volume

- De données sur le serveur : 100 MB / 500 MB
- De transfert par mois : 6 GB / 10 GB

Caractéristiques du service après-vente :

- Inclus dans le prix d'achat : 5 emails / 50 emails
- Coût d'une intervention : inconnu

4. Fournisseur : Web Technologies s.a.

Site : www.web.lu
Nom du service : Dedicated Hosting Windows / Linux

Serveur dédié : oui

Sécurité

- Chiffrement des données lors des échanges : oui
- Garantie de la bande passante : non
- Uptime garanti : non
- Duplication des données : manuelle

Fiabilité du fournisseur de la solution

- Durée du préavis lors de la rupture du contrat : inconnu
- Année de la commercialisation de la solution : 2000
- Signalisation de la localisation du serveur : non

Coût

- Coût initial : 0
- Coût par mois : 250 euros / 200 euros

Volume

- De données sur le serveur : 40 GB
- De transfert par mois : inconnu

Caractéristiques du service après-vente :

- Inclus dans le prix d'achat : inconnu
- Coût d'une intervention : inconnu

5. Fournisseur : e-hosting

Site : http://www.e-hosting.lu/hosting.php
Nom du service : Commercial Sites Pro1 / Pro3

Serveur dédié : non

Sécurité

- Chiffrement des données lors des échanges : non
- Garantie de la bande passante : non
- Uptime garanti : non
- Duplication des données : inconnu

Fiabilité du fournisseur de la solution

- Durée du préavis lors de la rupture du contrat : inconnu
- Année de la commercialisation de la solution : inconnu
- Signalisation de la localisation du serveur : non

Coût
- Coût initial : 0
- Coût par mois : 35 euros / 51 euros

Volume
- De données sur le serveur : 100 / 250
- De transfert par mois : 4 GB / 8 GB

Caractéristiques du service après-vente :
- Inclus dans le prix d'achat : inconnu
- Coût d'une intervention : inconnu

6. Fournisseur : e-hosting

Site : http://www.e-hosting.lu/hosting.php
Nom du service : A-1000 / Saphira PIII

Serveur dédié : oui

Sécurité
- Chiffrement des données lors des échanges : inconnu
- Garantie de la bande passante : non
- Uptime garanti : non
- Duplication des données : non / oui (raid 1)

Fiabilité du fournisseur de la solution
- Durée du préavis lors de la rupture du contrat : inconnu
- Année de la commercialisation de la solution : inconnu
- Signalisation de la localisation du serveur : non

Coût
- Coût initial : 175 euros / 399 euros
- Coût par mois : 175 euros / 399 euros

Volume
- De données sur le serveur : 40 GB
- De transfert par mois : 5 GB / 10 GB

Caractéristiques du service après-vente :
- Inclus dans le prix d'achat : inconnu
- Coût d'une intervention : inconnu

7. Fournisseur : Visual Online

Site : www.vo.lu

Nom du service : Basic / XXL

Serveur dédié : non

Sécurité
- Chiffrement des données lors des échanges : non
- Garantie de la bande passante : non
- Uptime garanti : non
- Duplication des données : inconnu

Fiabilité du fournisseur de la solution
- Durée du préavis lors de la rupture du contrat : 15 jours
- Année de la commercialisation de la solution : 1998
- Signalisation de la localisation du serveur : non

Coût
- Coût initial : 75 euros
- Coût par mois : 32 euros / 111 euros

Volume
- De données sur le serveur : 100 MB / 500 MB
- De transfert par mois : inconnu

Caractéristiques du service après-vente :
- Inclus dans le prix d'achat : inconnu
- Coût d'une intervention : un an de support par email : 20 euros

8. Fournisseur : LuxWebMaster.com

Site : www.luxwebmaster.com
Nom du service : Basic / Pro

Serveur dédié : non

Sécurité
- Chiffrement des données lors des échanges : non / oui
- Garantie de la bande passante : non
- Uptime garanti : 99%
- Duplication des données : non

Fiabilité du fournisseur de la solution
- Durée du préavis lors de la rupture du contrat : 0 jours
- Année de la commercialisation de la solution : 2003
- Signalisation de la localisation du serveur : non

Coût
- Coût initial : *en attente de réponse*
- Coût par mois : *en attente de réponse*

Volume
- De données sur le serveur : 50 MB / 1500 MB
- De transfert par mois : 3 GB / 10 GB

Caractéristiques du service après-vente :
- Inclus dans le prix d'achat : mail
- Coût d'une intervention : inconnu

9. Fournisseur : host.lu

Site : www.host.lu
Nom du service : Basic / Advanced

Serveur dédié : non

Sécurité
- Chiffrement des données lors des échanges : non
- Garantie de la bande passante : non
- Uptime garanti : non
- Duplication des données : non

Fiabilité du fournisseur de la solution
- Durée du préavis lors de la rupture du contrat : inconnu
- Année de la commercialisation de la solution : 2001
- Signalisation de la localisation du serveur : non

Coût
- Coût initial : 0
- Coût par mois : 35 euros / 70 euros

Volume
- De données sur le serveur : 50 MB / 150 MB
- De transfert par mois ; 2 GB / 4 GB

Caractéristiques du service après-vente :
- Inclus dans le prix d'achat : mail inclu
- Coût d'une intervention : inconnu

10. Fournisseur : Focus.lu

Site : www.focus.lu
Nom du service : WebSpace Gold / Dedicated Server

Serveur dédié : non / oui

Sécurité
- Chiffrement des données lors des échanges : non / oui
- Garantie de la bande passante : non
- Uptime garanti : 99.99%

- Duplication des données : triple

Fiabilité du fournisseur de la solution
- Durée du préavis lors de la rupture du contrat : inconnu
- Année de la commercialisation de la solution : 1999
- Signalisation de la localisation du serveur : non

Coût
- Coût initial : 0
- Coût par mois : 12 euros / 65 euros

Volume
- De données sur le serveur : 20 MB / > 16 GB
- De transfert par mois : illimité / 100 GB

Caractéristiques du service après-vente :
- Inclus dans le prix d'achat : inconnu
- Coût d'une intervention : inconnu

11. Fournisseur : LuxHosting

Site : www.luxhosting.lu
Nom du service : Starter / Millenium

Serveur dédié : non

Sécurité
- Chiffrement des données lors des échanges : non
- Garantie de la bande passante : non
- Uptime garanti : 99.9%
- Duplication des données : manuelle, mais possible
- Excellente clareté de la politique de sécurité : courant de secours, monitoring, …

Fiabilité du fournisseur de la solution
- Durée du préavis lors de la rupture du contrat : aucun
- Année de la commercialisation de la solution : 1999
- Signalisation de la localisation du serveur : oui

Coût
- Coût initial : 0
- Coût par mois : 6 euros / 25 euros

Volume
- De données sur le serveur : 250 MB / 2 GB
- De transfert par mois : 3 GB / 20 GB

Caractéristiques du service après-vente :
- Inclus dans le prix d'achat : inconnu
- Coût d'une intervention : inconnu

Fournisseur	Nom	Serveur dédié	Uptime garanti	Backup	Cout (euros) / mois	Volume sur le serveur (MB)	Transfert (GB) / mois
Tiscali	Serveur partagé	Non	Non	Non	?	25	?
Generity	Basic	Non	Non	Non	2	60	Illimité
Generity	Ultra	Non	Non	Non	10	300	Illimité
Web Tech.	Basic	Non	Non	Non	35	100	6
Web Tech.	Business	Non	Non	Quotidien	80	500	10
e-hosting	Pro1	Non	Non	Non	35	100	4
e-hosting	Pro3	Non	Non	Non	51	250	8
Visual Online	Basic	Non	Non	Non	32	100	?
Visual Online	XXL	Non	Non	Non	111	500	?
LuxWebMaster	Basic	Non	99%	Non	?	50	3
LuxWebMaster	Pro	Non	99%	Non	?	1500	10
Host.lu	Basic	Non	Non	Non	35	50	2
Host.lu	Advanced	Non	Non	Non	70	150	4
Focus.lu	WebS. Gold	Non	99.99%	Triple	12	20	Illimité
LuxHosting	Starter	Non	99.9%	Manuelle	6	250	3
LuxHosting	Millenium	Non	99.9%	Manuelle	25	2.000	20
Tiscali	Serveur dédié	Oui	Non	Oui	?	Inconnu	?
Web Tech.	Windows	Oui	Non	Manuelle	250	40.000	?
Web Tech.	Linux	Oui	Non	Manuelle	200	40.000	?
e-hosting	A-1000	Oui	Non	Raid 1	175	40.000	5
e-hosting	Saphira PIII	Oui	Non	Raid 1	399	40.000	10
Focus.lu	Dedicated S.	Oui	99.99%	Triple	65	16.000	100

3. Annexe C - Bases de données - Etude de l'existant

Critères

Fabriquant
Nom du produit
Version du produit
Mode d'exploitation
En terme de localisation externe de la solution :

- Chiffrement des données lors des échanges (o/n)
- Fiabilité du fournisseur de la solution
  - Durée du préavis lors de la rupture du contrat
  - Nombre de requêtes concurrentes limitées (o/n)
  - Nombre de requêtes par mois limitées (o/n)
  - Année de la commercialisation de la solution
- Rapidité de la connexion (Mb/s)

Pour l'achat du software : type de software

- Libre / Gratuit
- Propriétaire
  - Coût de l'achat du software initial
  - Coût du software par utilisateur par an

Pour la location du software :

- Coût initial
- Coût par utilisateur par mois

Caractéristiques du service après-vente :

- Inclus dans le prix d'achat (oui / non / durée)
- Coût d'une intervention

Fabriquant : Oracle **(www.oracle.com)**

Nom du produit : Oracle
Version du produit : Entreprise Edition / Personnal Edition / Lite
Mode d'exploitation : Intermédiaire 1
Type de software : Propriétaire

- Coût de l'achat du software (par utilisateur) : $800 / $400 / $100

Caractéristiques du service après-vente :

- Inclus dans le prix d'achat : support téléphonique inclut
- Coût d'une intervention : inconnu

Fabriquant : Borland (www.borland.com)

Nom du produit : Interbase
Version du produit : Desktop Licence / Server Licence
Mode d'exploitation : Intermédiaire 1
Type de software : Propriétaire

- Coût de l'achat du software initial : $60 / $200

Caractéristiques du service après-vente :

- Inclus dans le prix d'achat : oui (30 jours)
- Coût d'une intervention : inconnu

Fabriquant : IBM (www.ibm.com)

Nom du produit : IBM DB2
Version du produit : Server Edition 8.1 / Personal Edition 8.1
Mode d'exploitation : Intermédiaire 1
Type de software : Propriétaire

- Coût de l'achat du software initial : $33.000 / $460

Caractéristiques du service après-vente :

- Inclus dans le prix d'achat : oui (1 an)

Fabriquant : Microsoft (www.microsoft.com)

Nom du produit : Microsoft Access
Version du produit
Mode d'exploitation : Intermédiaire 1
Type de software : Propriétaire

- Coût de l'achat du software initial : $230

Caractéristiques du service après-vente :

- Inclus dans le prix d'achat : inconnu
- Coût d'une intervention : inconnu

Fabriquant : FileMaker (www.filemaker.com)

Nom du produit : FileMaker Pro
Version du produit : Pro / Unlimited
Mode d'exploitation Intermédiaire 1
Type de software : propriétaire

- Coût de l'achat du software initial : $300 / $1000

Caractéristiques du service après-vente :

- Inclus dans le prix d'achat : 1 appel
- Coût d'une intervention : $50 par appel

Fabriquant : Sybase (www.sybase.com)

Nom du produit : Sybase
Version du produit : Adaptive Server Enterprise For SME 12.5
Mode d'exploitation Intermédiaire 1
Type de software : Propriétaire

- Coût de l'achat du software initial : $1500
- Coût du software par utilisateur : $200

Caractéristiques du service après-vente :

- Inclus dans le prix d'achat : non
- Coût d'une intervention : inconnu

Fabriquant : IBPhoenix Services (www.ibphoenix.com)

Nom du produit : Firebird
Version du produit : 1.0
Mode d'exploitation Intermédiaire 1
Type de software : Libre
Caractéristiques du service après-vente :

- Inclus dans le prix d'achat : non
- Coût d'une intervention : 1 mois d'email illimité : $750

Fabriquant : MySQL (www.mysql.com)

Nom du produit : MySQL
Version du produit : MySQL 4.0
Mode d'exploitation : Intermédiaire 1

Type de software : Libre
Caractéristiques du service après-vente :

- Inclus dans le prix d'achat : non
- Coût d'une intervention :
  - Mail : $1500 / an

Fabriquant : PostgreSQL (www.postgresql.org)

Nom du produit : PostgreSQL
Version du produit : 7.3
Mode d'exploitation : Intermédiaire 1
Type de software : Libre
Service après-vente :

- Inclus dans le prix d'achat : non
- Coût d'une intervention :
  - Mail et téléphone : $200 / mois

Solution 2 : Localisation de la solution en externe, compétences de gestion externes, logiciel loué, matériel inclus

Fabriquant : Verio (www.verio.com)

Nom du produit : Oracle
Version du produit : Oracle8i
Mode d'exploitation : 25
Chiffrement des données lors des échanges : non
Fiabilité du fournisseur de la solution

- Durée du préavis lors de la rupture du contrat : Aucune pour le client, inconnue pour le fournisseur
- Nombre de requêtes concurrentes limitées : 10
- Nombre de requêtes par mois : illimitées
- Année de la commercialisation de la solution : 1998
- Rapidité de la connexion (Mb/s) : inconnue

Pour la location du software :

- Coût initial : $250
- Coût par utilisateur par mois : $50 (5 utilisateurs)

Caractéristiques du service après-vente :

- Inclus dans le prix d'achat : non
- Coût d'une intervention : pas d'intervention directe. Passer directement via oracle. Un service d'aide via mail est disponible.

Fabriquant : QuickBase (www.quickbase.com)

Nom du produit : QuickBase
Version du produit : For Small Business / For Workgroups
Mode d'exploitation : All Externe

Chiffrement des données lors des échanges : oui
Fiabilité du fournisseur de la solution

  - Durée du préavis lors de la rupture du contrat : 30 jours
  - Nombre de requêtes concurrentes limitées : non
  - Nombre de requêtes par mois limitées : non
  - Année de la commercialisation de la solution : 1999
- Rapidité de la connexion (Mb/s) : inconnue

Pour la location du software : For Small business / For Workgroups

- Coût initial : $0
- Coût par utilisateur par mois : $ [3 – 10] / $25

Caractéristiques du service après-vente :

- Inclus dans le prix d'achat : support par email gratuit
- Coût d'une intervention : inconnu

Fabriquant : eCriteria (www.ecriteria.net)

Nom du produit : eCriteria
Version du produit : Standard / Enterprise
Mode d'exploitation : All Externe

Chiffrement des données lors des échanges : Standard : non, Enterprise : oui
Fiabilité du fournisseur de la solution

- Durée du préavis lors de la rupture du contrat : 15 jours
- Nombre de requêtes concurrentes limitées : Standard : 1 utilisateur, Enterprise : 25 utilisateurs
- Nombre de requêtes par mois limitées : oui
- Année de la commercialisation de la solution : 1999

Rapidité de la connexion (Mb/s) : inconnue

Pour la location du software :

- Coût initial : $0
- Coût par mois : Standard : $5, Entreprise : $40

Caractéristiques du service après-vente : inexistant en tant que tel. Support par email gratuit.

Fabriquant : Rent-a-db (www.rent-a-db.com)

Nom du produit : Rent-a-db
Version du produit : N/A
Mode d'exploitation : All Externe

Chiffrement des données lors des échanges : non
Fiabilité du fournisseur de la solution

- Durée du préavis lors de la rupture du contrat : aucun
- Nombre de requêtes concurrentes limitées : oui
- Nombre de requêtes par mois limitées : oui
- Année de la commercialisation de la solution : 2001
- Rapidité de la connexion (Mb/s) : inconnue

- Duplication des données : non

Pour la location du software :

- Coût initial : $0
- Coût par utilisateur par mois : $0

Caractéristiques du service après-vente :

- Inclus dans le prix d'achat : non
- Coût d'une intervention

Fabriquant : personable (www.personable.com)

Nom du produit : MS Access 2000
Version du produit : MS Access 2000 Multilanguage Version
Mode d'exploitation : All Externe

Chiffrement des données lors des échanges : non
Fiabilité du fournisseur de la solution

- Durée du préavis lors de la rupture du contrat : inconnue
- Nombre de requêtes concurrentes limitées : non
- Nombre de requêtes par mois limitées : non
- Année de la commercialisation de la solution : 2000

Rapidité de la connexion (Mb/s) : inconnue

Pour la location du software :

- Coût initial : $25 par utilisateur
- Coût par mois : $33 par utilisateur

Caractéristiques du service après-vente :

- Inclus dans le prix d'achat : aide via email illimité
- Coût d'une intervention : inconnu

Fabriquant : personable (www.personable.com)
Nom du produit : SvW Data Keeper
Version du produit : SvW Data Keeper
Mode d'exploitation : All Externe

Chiffrement des données lors des échanges : non
Fiabilité du fournisseur de la solution

- Durée du préavis lors de la rupture du contrat : inconnue
- Nombre de requêtes concurrentes limitées : non
- Nombre de requêtes par mois limitées : non
- Année de la commercialisation de la solution : 2000

Rapidité de la connexion (Mb/s) : inconnue

Pour la location du software :

- Coût initial : $25 par utilisateur
- Coût par mois : $20 par utilisateur

Caractéristiques du service après-vente :

- Inclus dans le prix d'achat : aide via email illimité
- Coût d'une intervention : inconnu

Fabriquant : Primasoft (www.primasoft.com)
Nom du produit : Web dB Server
Version du produit : Web dB Server Personal Account / Corporate Account

Mode d'exploitation : All Externe

Chiffrement des données lors des échanges : non
Fiabilité du fournisseur de la solution

- Durée du préavis lors de la rupture du contrat : inconnu
- Nombre de requêtes concurrentes limitées : non
- Nombre de requêtes par mois limitées : non
- Année de la commercialisation de la solution : inconnue

Rapidité de la connexion (Mb/s) : inconnue

Pour la location du software :

- Coût initial : $0
- Coût par utilisateur par mois : Personnal : $30 / Corportate : $250

Caractéristiques du service après-vente :

- Inclus dans le prix d'achat : inconnu
- Coût d'une intervention : inconnu